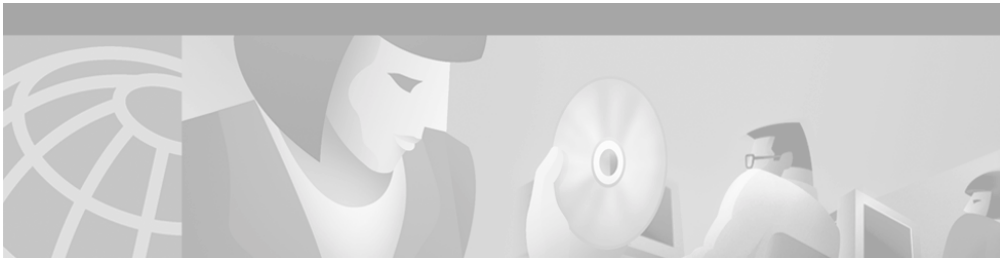
User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7814092=
Text Part Number: 78-14092-01

CONTENTS

APPENDIX B



Preface

This manual describes the Wireless LAN Solution Engine and provides instructions for using it.

Audience

This document is for system administrators responsible for managing a wireless network who are familiar with some of the concepts and terminology of Ethernet and wireless local area networking.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font

Item	Convention
Menu items and button names	**boldface** font
Selecting a menu item	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Note Although every effort has been made to validate the accuracy of the information in the printed and electronic documentation, you should also review the [product] documentation on Cisco.com for any updates.

The following additional documentation is available:

Paper Documentation

- *Installation and Configuration Guide for the CiscoWorks 1105 Wirless LAN Solution Engine*
- *Quick Start Guide for the CiscoWorks 1105 Wirleless LAN Solution Engine*
- *Release Notes for the CiscoWorks 1105 Wireless LAN Solution Engine*
- *Regulatory Compliance and Safety Information for the CiscoWorks 1105 Wireless LAN Solution Engine*

Online Documentation

- Online help—Access the online help by clicking on the Help tab.
- PDF for:
  - *Installation and Configuration Guide for the CiscoWorks 1105 Wirless LAN Solution Engine*
  - *Quick Start Guide for the CiscoWorks 1105 Wirleless LAN Solution Engine*
  - *Regulatory Compliance and Safety Information for the CiscoWorks 1105 Wireless LAN Solution Engine*

Note Adobe Acrobat Reader 4.0 is required.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Feedback** at the top of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

Getting Started with the Wireless LAN Solution Engine

The following topics provide an overview of the Wireless LAN Solution Engine (WLSE) and assistance in getting started:

Overview of the Wireless LAN Solution Engine

The WLSE is a hardware and software solution for managing Cisco wireless devices. The WLSE has the following major features:

- Configuration

  Allows you to apply a set of configuration changes to a group of access points and connected switch ports.

- Reporting

  Allows you to display reports for tracking device, client and security information. Reports can be emailed, printed, or exported.

- Fault and Policy Monitoring

  Provides device monitoring for fault and performance conditions, monitoring of LEAP server responses, and monitoring of policy misconfigurations.

The WLSE works by gathering fault, performance, and configuration information about the Cisco wireless devices that it discovers in your network. The WLSE allows you to manage the discovered devices. You can customize configuration templates and apply them, display reports on managed devices and wireless clients, and monitor device faults.

When you log in to the WLSE, a dashboard appears with the following tabs:

Tab	Allows you to ...	See...
Faults	Display device faults, specify fault thresholds, specify policies, and enable syslog and traps.	Fault Monitoring, page 2-1.
Configure	Create and apply configuration templates and manage jobs.	Configuring Devices, page 3-1.
Reports	Run, view and email reports.	Using Reports, page 4-1.
Administration	Perform administrative tasks such as discovering devices, managing user profiles, and managing the appliance.	Performing Administrative Tasks, page 5-1.

Date and Time Display on the WLSE

The WLSE uses browser (client) time in most of its displays. The format of timestamps depends on the browser you are using:

- In Internet Explorer, the timestamp is date, tim (hours:minutes:seconds), timezone, and year; for example:

  Mon Mar 25 13:29:21 PST 2002

- In Netscape Navigator, the timestamp is date, time (hours:minutes:seconds), offset from GMT/UTC, timezone, and year; for example:

  Mon Mar 25 13:29:21 GMT-0800 (Pacific Standard Time) 2002

In some WLSE tables, the timestamp is *hours*:*minutes*:*seconds month*/*day*/*year*; for example, 19:23:44 06/29/2002. The time is browser (client) time.

The WLSE's system time is Universal Coordinated Time (UTC), and UTC is used in certain displays, such as the Discovery Run Log. To display or reset the system time, see the instructions in the *Hardware Installation and Configuration Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

Getting Started

Before you can use WLSE monitoring, configuration, and reporting, you must set up your devices, initiate discovery, and move devices into the managed state. To get started, follow the directions in the *Quick Start Guide* or use the following task list.

Task	Description and References
1. Set up devices (access points, bridges, routers, switches, and LEAP servers).	See Set Up Devices, page 5-4 for details.
2. Log in to the WLSE using a Web browser.	Enter the WLSE's IP address, followed by:1741; for example, http://209.165.202.128:1741.
3. Enter device credentials.	Device community strings must be entered on the WLSE. See Setting Device Credentials, page 5-17. For access point configuration tasks, the HTTP username and password must be entered on the WLSE. See Specify the HTTP Username and Password, page 5-20.
4. Initiate discovery from the WLSE or import devices from a file or from CiscoWorks.	If you are using discovery from the WLSE, add seed devices and enable discovery. You can initiate an immediate one-time discovery or schedule discovery for a later time. See Managing Device Discovery, page 5-2.
5. Verify the discovery.	On the WLSE, verify that devices were discovered. See View Discovery History and Status, page 5-12.

Task	Description and References
6. Set device state to “managed” and run inventory polling.	You must move devices to the managed state on the WLSE before you can use configuration, reporting, and monitoring features. After moving devices to the managed state, you should perform an immediate inventory polling to obtain device information needed to use such WLSE features as reports and automatic grouping. See Using Discovery and Managing Devices, page 5-2.
7. Create other users and user roles as needed.	The WLSE has one predefined user (the system administrator) and four predefined user roles. User roles are used to specify the WLSE functions a given user can have access to. To allow other users access to the WLSE, the system administrator must add users. The system administrator can also create roles to customize user access. SeeAdministering Users, page 5-60.

Logging Out

To log out from the WLSE, click **Logout** in the upper right corner of the window.

Fault Monitoring

The Faults tab displays information to help you monitor your devices. All the device information shown under this tab is polled from the devices in your network.

Following are the subtabs under Faults:

Note Some of the subtabs may not be visible to some users.

- **Display Faults**—See Displaying Faults, page 2-1
- **Specify Fault Thresholds**—See Specifying Fault Thresholds, page 2-7
- **Specify Policies**—See Specifying Policies, page 2-13
- **Fault Forwarding**—See Forwarding Faults, page 2-15

Displaying Faults

This window displays device fault information. A fault is an abnormal condition that occurs when a system component exceeds a performance threshold or is not functioning properly. (See Specifying Fault Thresholds, page 2-7 to set threshold levels.)

A fault can also occur when a system policy is violated. (See Specifying Policies, page 2-13 to set policies.)

Displayed fault information is retained by default for 30 days. To change the default, see Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults > Display Faults**. The Fault window appears.

Step 2 Use the Filter: bar to display the faults you want to view:

Table 2-1 Display Faults Filter Bar

Field	Description
Devices	From the list, select the device type whose fault summary you want to display.

Table 2-1 Display Faults Filter Bar (continued)

Field	Description
Severity	From the list, select the severity from P1, which is the highest severity level to P5, which is the lowest severity level, to display: • P1—Severity P1 faults. • P1-P2—Severity P1 and P2 faults. • P1-P3—Severity P1 through P3 faults. • P1-P4—Severity P1 through P4 faults. • P1-P5—Severity P1 through P5 faults. • All—Severity P1 through P5 faults, and faults that have been cleared.
State	From the list, select a states to display: • All—Faults in all states are displayed. • Active—Faults are active (current) and have not been acknowledged. • Acknowledged—Faults that are active and have been acknowledged. • Cleared—Faults that have been cleared (no longer in an Active or Acknowledged state).

Step 3 Click **Apply**. The following table appears:

Note If no data is displayed in the table, there are no faults for your filtering selection to report.

Table 2-2 Display Faults Table

Column	Description
IP Address	The device IP address. Click to see the device's summary report. For: • Access Points— see Displaying an AP Summary Report, page 4-11. • Switches— see Displaying a Switch Summary Report, page 4-17. • Routers— see Displaying a Router Summary Report, page 4-19.
Hostname	The device for which the fault is reported. Click to see the device's summary report. For: • Access Points— see Displaying an AP Summary Report, page 4-11. • Switches— see Displaying a Switch Summary Report, page 4-17. • Routers— see Displaying a Router Summary Report, page 4-19.
Family	The product family.
Product	The product name.
Type	The device or the sub-device component.

Table 2-2 Display Faults Table (continued)

Column	Description
Description	A description of the fault. Click to see fault details. See Viewing Fault Details, page 2-6.
Severity	The fault severity level.
State	The operational state of the device.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Date and Time Display on the WLSE, page 1-2. Click to see fault details. See Viewing Fault Details, page 2-6.

Step 4 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 5 To acknowledge (change the state from Active to Acknowledged):

- A single fault, check it, then click **Acknowledge**.
- All faults, click **Select All**, then click **Acknowledge**.

Step 6 To unacknowledge (change the state from Acknowledged to Active):

- A single fault, check it, then click **Unacknowledged.**
- All faults, click **Select All,** then click **Unacknowledged**.

Related Topics

- Specifying Fault Thresholds, page 2-7
- Specifying Policies, page 2-13
- Forwarding Faults, page 2-15

Viewing Fault Details

The following tables are displayed in the Fault Details window.

To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Fault details for

Column	Description
IP	The device IP address.
Name	The device hostname.
Family	The device family.
Product	The product name.
Type	The device or the device sub-entity (which could include a logical entity, such as software or a service) in which the fault is found. **Note** If the Type is a sub-entity, additional columns appear with keys and values to help identify the precise sub-entity. These additional keys and values are MIB variables.

Conditions

Column	Description
Name	The fault condition.
State	The state of the device.
Severity	The fault severity level.

Column	Description
Description	A description of the fault.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Date and Time Display on the WLSE, page 1-2.

Fault History

Column	Description
State	The state of the device.
Severity	The fault severity level.
Description	A description of the fault.
Change	A description of the state change.
Timestamp	Indicates the time, based on the client browser, that the state of the device last changed. See Date and Time Display on the WLSE, page 1-2.
By	Displays the username of the person who changed the fault state. If the fault state has not been acknowledged, nothing is displayed in this column.

Specifying Fault Thresholds

This window allows you to set polling and exception threshold values collected from the devices you are monitoring.

The threshold values you set in this window will determine how the faults are displayed in the **Faults** > **Display Faults** subtab.

Note Your login determines whether you can use this option.

The Specify Fault Threshold window has the following options:

- **Access Point**—See Setting Access Point Fault Thresholds, page 2-8.
- **Switch**—See Setting Switch Fault Thresholds, page 2-10.
- **LEAP**—See Setting LEAP Server Response Time, page 2-12.

Related Topics

- Displaying Faults, page 2-1
- Specifying Policies, page 2-13
- Forwarding Faults, page 2-15

Setting Access Point Fault Thresholds

Using this option, you can set up thresholds for access point faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Select **Faults > Specify Fault Thresholds**. The Fault threshold window appears.

Step 2 Select **Access Point** in the left pane and the menu expands.

Step 3 Select any of the following to set values for:

- SNMP Reachable—Go to Step 4.
- RF port status—Go to Step 4.
- RF port utilization—Go to Step 6.
- RF port packet errors—Go to Step 6.
- RF port WEP errors—Go to Step 6.
- RF port FCS errors—Go to Step 6.
- Ethernet port status—Go to Step 4.

- Ethernet port utilization—Go to Step 6.
- Ethernet port packet errors—Go to Step 6.

Step 4 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 5 Continue to Step 7.

Step 6 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.

Field	Description
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 7 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Setting Switch Fault Thresholds

Using this option, you can set up thresholds for switch faults. When the thresholds are exceeded, faults are generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Select **Faults > Specify Fault Threshold**. The Fault threshold window appears.

Step 2 Select **Switch** in the left pane and the menu expands.

Step 3 Select any of the following to set values for:

- SNMP Reachable —Go to Step 4.
- CPU utilization—Go to Step 6.
- Memory utilization—Go to Step 6.
- Port Status—Go to Step 4.
- Port Utilization—Go to Step 6.
- Module Status—Step 4.

Step 4 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling Interval	From the list, select the polling interval.
Settings	
Down	From the list, select the severity level and the number of polling cycles before the status is Down.
Up	From the list, select the number of polling cycles before the fault is cleared and the status is Up.

Step 5 Go to step Step 7.

Step 6 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the percentage, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the percentage, and the number of polling cycles before the status is OK.

Step 7 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Setting LEAP Server Response Time

Using this option, you can set up a threshold for LEAP server response time. When the threshold is exceeded, a fault is generated and can be viewed under **Faults > Display Faults**.

Procedure

Step 1 Select **Faults > Specify Fault Threshold**. The LEAP Server:Response Time threshold window appears.

Step 2 Select **LEAP** in the left pane and the menu expands.

Step 3 Complete the following:

Field	Description
Enable	Check to enable a threshold for this component.
Polling Interval	From the list, select the polling interval.
Settings	
Overloaded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Overloaded.
Degraded	From the list, select the severity level, the response time, and the number of polling cycles before the status is Degraded.
OK	From the list, select the severity level, the response time, and the number of polling cycles before the status is OK.

Step 4 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Specifying Policies

This is window allows you to activate or deactivate a set of pre-defined policies for access points.

The policies you set in this window will determine how some of the faults are displayed in the **Faults** > **Display Faults** subtab.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Faults** > **Specify Policies**. The Access Point window appears.

Step 2 In the left pane, select the variable for which you want to set a policy.

- SSID—Go to Step 3
- Broadcast SSID Disabled—Go to Step 6
- WEP Enabled—Go to Step 6
- LEAP Enabled—Go to Step 6
- WEP Key Length—Go to Step 8
- HTTP Disabled—Go to Step 6
- Telnet Disabled—Go to Step 6
- User Manager Enforced—Go to Step 6
- HTTP Authentication—Go to Step 6

Step 3 To activate the policy, do the following:

Field	Description
Verify	Check if you want to verify that SSID is enabled.
Polling Interval	From the list, select the polling interval.

Field	Description
Severity	From the list, select a severity level to associate with this policy.
Enter ssid	Enter the unique identifier used by client devices to associate with the access point. Any alphanumeric character up to 32 characters long.

Step 4 Click **Add** to add the SSID to the list, then go to Step 9.

Step 5 To remove an SSID from the list, select it, click **Remove**, then go to Step 9**.**

Step 6 Complete the following:

Field	Description
Verify	Check if you want to verify one of the following: • Broadcast SSID is disabled • WEP is enabled • LEAP is enabled • HTTP is disabled • Telnet is disabled • User Manager Capabilities are enforced • HTTP authentication
Polling Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.

Step 7 Go to Step 9.

Step 8 Complete the following:

Field	Description
Verify	Check if you want to verify the WEP key length.
Polling Interval	From the list, select the polling interval.
Severity	From the list, select a severity level to associate with this policy.
WEP Key Length	Select to indicate the bit length.

Step 9 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to set the new entries.

Related Topics

- Displaying Faults, page 2-1
- Specifying Fault Thresholds, page 2-7
- Forwarding Faults, page 2-15

Forwarding Faults

This window allows you to set SNMP traps to enable north-bound exception notification to specified hosts, issue syslog messages to selected syslog servers, and send exception notification email to selected users.

This section has the following options:

- Setting Trap Notification
- Setting Syslog Notification
- Emailing Faults

Note Your login determines whether you can use this option.

Related Topics

- Displaying Faults, page 2-1
- Specifying Fault Thresholds, page 2-7
- Specifying Policies, page 2-13

Setting Trap Notification

This option allows you to enable the WLSE to send north-bound exception notification to one or more SNMP trap receivers. The exception notification contains information such as device name and IP, fault number, timestamp, exception severity, and a message describing the problem.

Before You Begin

Make sure your SNMP trap receiver's trap receiving daemon is set to the correct port. The default port is set to 162.

Procedure

Step 1 Select **Faults > Fault Forwarding.** The Fault Forwarding dialog box appears.

Step 2 Complete the following:

Field	Description
Trap	Check to enable trap notification.
Port	Enter the port number if different from the default of 162.
Host	Enter the hostname/IP of the SNMP trap receiver to which you want to send SNMP trap notification.
Community	Enter the community string.

Step 3 If you want a different host to receive trap notification, click **add row**. There is no limit to the number you can enter.

To delete a row, click **delete,** next to the row you want to remove.

Step 4 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Syslog Notification, page 2-17
- Emailing Faults, page 2-18

Setting Syslog Notification

This option allows you to send syslog messages to selected syslog servers. The messages contain information such as device name and IP, fault number, date and time, exception severity, and a message about what is wrong.

Before You Begin

Make sure your syslog server is turned on to be able to receive messages from the Wireless LAN Solution Engine. Also make sure that the receiving process is configured to receive messages from remote hosts (for example, start syslogd with -r option on some unix versions).

Procedure

Step 1 Select **Faults > Fault Forwarding**. The Fault Forwarding dialog box appears.

Step 2 Complete the following:

Field	Description
Syslog	Check to send syslog messages to designated syslog servers.
Enter Syslog host names	Enter the hostname/IP for the syslog servers. Names must be separated by a space, a comma, a semicolon, or a new line.

Step 3 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Trap Notification, page 2-16
- Emailing Faults, page 2-18

Emailing Faults

The emailed exception notification contains information such as device name and IP, fault number, exception severity, and a message about what is wrong

Procedure

Step 1 Select **Faults > Fault Forwarding**. The Fault Forwarding dialog box appears.

Step 2 Complete the following:

Field	Description
Email	Check to enable email notification of exception information.
Enter email addresses	Enter the email addresses of users you want to receive exception notification. Addresses must be separated by a space, a comma, a semicolon, or a new line.
Priority	From the list, select the priority of the exceptions you want these uses to receive.

Step 3 If you want a different group of users to receive different priority level exceptions, click **add row** to add another set of email addresses. There is no limit to the number of email addresses you can enter.

Step 4 Click **Reset** to refresh any fields you have changed but want to restore, or **Apply** to save your settings.

Related Topics

- Setting Trap Notification, page 2-16
- Setting Syslog Notification, page 2-17

CHAPTER 3

Configuring Devices

The Configure tab allows you to view, create, copy, edit, and delete configuration templates and apply them to large numbers of devices at a time.It also allows you to schedule a configuration job and to check on the job's status.

Following are the subtabs under Configure:

Note Some of the subtabs may not be visible to some users.

- **Templates**—See Using the Templates, page 3-1.
- **Jobs**—See Managing Configuration Jobs, page 3-92.

Using the Templates

This is window allows you to create, modify, and delete configuration templates.

The topics covered in this section are:

Related Topic

Managing Configuration Jobs, page 3-92

Template Choices

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

When you create or edit a configuration template, the following choices appear in the left pane of the Templates window:

1. **Template Name**—See Naming the Template, page 3-3.
2. **Template Categories**

Note Any or all of the template categories can be completed in any order.

   - **Express Template**—See Using Express Template, page 3-3.
   - **Association**—See Setting Up Association, page 3-7.
   - **Ethernet**—See Configuring the Ethernet Port, page 3-31.
   - **Radio**—See Configuring the Radio, page 3-36.
   - **Security**—See Defining the Security Settings, page 3-51.
   - **Services**—See Configuring Services, page 3-60.
   - **Events**—See Configuring Events, page 3-79.
   - **Custom Values**—See Configuring Custom Values, page 3-85.
3. **Preview**—See Previewing the Template, page 3-89.
4. **Finish**—See Finishing the Template, page 3-89.

Naming the Template

This option enables to you to name the template.

Procedure

Note Clicking **Clear** removes all the entries you have made.

Step 1 Select **Template Name**. The Template Name dialog box appears:

Field	Description
Name	Enter a name for the template. See Naming Guidelines, page A-1.
Description	Enter a description of the purpose of the template. See Naming Guidelines, page A-1

Step 2 Select a template category. (For additional information, see Template Categories, page 3-2.)

Using Express Template

Use this option if you need to set up an access point quickly with a simple configuration. This will allow you to enter all the access point's essential settings for basic operation.

Procedure

Step 1 Select **Express Template**. The Express dialog box displays in the right pane:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-1 Express Template Settings

Field	Description
Configuration Server Protocol	Set this entry to match the network's method of IP address assignment. From the list, select one of the following options: • None-Static IP—Use this if your network does not have an automatic system for IP address assignment. • BOOTP—Use this if your network uses Bootstrap Protocol, in which IP addresses are hard-coded based on MAC addresses. • DHCP—Use this if your network uses Dynamic Host Configuration Protocol, in which IP addresses are "leased" for predetermined periods of time.
Default Subnet Mask	Enter an IP subnet mask to identify the subnetwork so the IP address can be recognized on the LAN. If DHCP or BOOTP is not enabled, this field is the subnet mask. If DHCP or BOOTP is enabled, this field provides the subnet mask only if no server responds to the access point's DHCP or BOOTP request.

Table 3-1 Express Template Settings (continued)

Field	Description
Default Gateway	Enter the IP address of your default Internet gateway. The entry 255.255.255.255 indicates no gateway.
Radio Service Set ID (SSID)	Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long. Several access points on a network or sub-network can share an SSID.

Table 3-1 Express Template Settings (continued)

Field	Description
Role in Network	From the list, select one of the following: • Access Point—Use this setting if the access point is connected to the wired LAN. • Repeater—Use this setting for access points not connected to the wired LAN. • Survey Client—Use this setting when performing a site survey for a repeater access point. When you select this setting, clients are not allowed to associate and the bridge's STP function is disabled. • Root Bridge—Use this setting to set a bridge as the root bridge. (One bridge in each group of bridges must be set as the root bridge). The root bridge cannot associate with another root bridge. • Non-Root Bridge w/ Client—Use this setting for non-root bridges that accept associations from client devices and for bridges acting as repeaters. A non-root bridge will only associate to another bridge (root or non-root). • Non-Root Bridge w/o Client—Use this setting for non-root bridges that should not accept associations from client devices. A non-root bridge (without clients) can connect to a wired LAN and only associates to another bridge (root or non-root).

Table 3-1 Express Template Settings (continued)

Field	Description
Ensure Compatibility with Cisco	From the list, select one of the following: • Enable—Use this setting to automatically configure the device to be compatible with other Cisco devices on your wireless LAN. • Disable—Use this setting to not automatically configure the device to be compatible with other Cisco devices on your wireless LAN.
Ensure Compatibility with 2MB/sec Clients	From the list, select one of the following: • Enable— Use this setting to operate at a maximum speed of two megabits per second. • Disable—Use this setting if you do not want devices to operate at a maximum speed of two megabits per second.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Association

Use this option to set up spanning tree protocol (STP) on bridges and to set up filtering to control the flow of data through the access point.

Procedure

Step 1 Select **Association**. The menu expands and the Association dialog box displays in the right pane.

Step 2 Select one of the following from the Association menu:

- Spanning Tree—Defining Spanning Tree Protocol, page 3-8.
- Address Filters—Defining Address Filters, page 3-11.
- Ethertype Filters—Defining Ethertype Filters, page 3-12.
- IP Protocol Filters—Defining IP Protocol Filters, page 3-16.
- IP Port Filters—Defining IP Port Filters, page 3-21.
- Advanced—Defining Advanced Associations, page 3-25.
- Port Assignments—Configuring Port Assignments, page 3-30.

Defining Spanning Tree Protocol

This option is used for only bridges.

Procedure

Step 1 Select **Association > Spanning Tree**. The Association: Spanning Tree Protocol dialog box appears.

Step 2 Click **see details** for information on which bridges this configuration is valid.

Step 3 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-2 Spanning Tree Protocol Settings

Field	Description
Spanning Tree Protocol (STP)	From the list, select one of the following: • Enable—Use this setting to enable STP on the bridge. • Disable—If you do not want STP enabled the bridge.
Root Configuration	
Priority (0-65535)	Enter a number to influence which bridge is designated the root bridge in the spanning tree. When bridges have the same priority setting, STP uses the bridges' MAC addresses as a tiebreaker. The bridge with the lowest priority setting is likely to be designated the root bridge in the tree.
Max Age (6-40 Seconds)	Enter the number of seconds to define how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt. For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BDPU from the root bridge in the spanning tree within 20 seconds.
Hello Time (1-10 Seconds)	Enter the number of seconds to define how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same.

Table 3-2 Spanning Tree Protocol Settings (continued)

Field	Description
Forward Delay (4-30 Seconds)	Enter the number of seconds to define how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree.
Port Configuration	
Path Cost (1-65535)	Enter a number to indicates the relative efficiency of a port's network link. A port with a high path cost is less likely to become a bridge's root port.
Priority (0-255)	Enter a number to influence whether STP designates a port as a bridge's root port. A port with a low priority setting is more likely to become a bridge's root port.
Enable	From the list, select one of the following for each port configured: • Enable—Use this setting to indicate whether the port participates in STP. (This determines whether the port blocks or forwards traffic.) • Disable—Use this setting to indicate that the port does not participate in STP.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Address Filters

Using this option, you can:

- Create a MAC address filter
- Remove a MAC address filter

Procedure

Step 1 Select **Association** > **Address Filters**. The Association: Address Filters dialog box appears.

Step 2 To add a new MAC address filter complete the following fields:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
New Destination MAC Address	Enter a destination MAC address by entering the address in one of the following ways: • With colons separating the character pairs (00:40:96:12:34:56, for example) • Without any intervening characters (004096123456, for example)
Allowed	Click to pass traffic to the MAC address.
Disallowed	Click to discard traffic to the MAC address.

Step 3 Click **Add** to add the MAC address to the Current MAC Address Filters list.

Step 4 To remove a MAC Address, select it from the Current MAC Address Filters list, then click **Remove**.

Step 5 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Ethertype Filters

Procedure

Step 1 Select **Association > Ethertype Filters.** The Association: Ethertype Filters dialog box appears.

Step 2 Using this option:

- Create new filters—See Creating New Ethertype Filters, page 3-12.
- Delete the Filters—See Deleting Ethertype Filters, page 3-14.

Using this option you can also:

- Create Special Cases —See Creating Special Cases, page 3-14.
- Delete Special Cases—See Deleting Special Cases, page 3-16.

Creating New Ethertype Filters

Procedure

Step 1 To create and enable protocol filters for the access point's Ethernet port, enter the following:

Table 3-3 Creating New Ethertype Filters Settings

Field	Description
Add New Ethertype Filter	
Set ID	Enter an identification number for the filter set.

Table 3-3 Creating New Ethertype Filters Settings (continued)

Field	Description
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add.** The new name is added to the Ethertype Filters list.

Step 3 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Ethertype Filters

Procedure

Step 1 To delete protocol filters for the access point's Ethernet port, select the set name from the Current Ethertype Filters list, then click **Delete**.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-4 Ethertype Filter Special Cases Settings

Field	Description
Special Cases	
Ethertype	Enter the Ethertype filter name.
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the Ethertype filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 3-4 Ethertype Filter Special Cases Settings (continued)

Field	Description
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Click **Add.** The new name is added to the list box.

Step 4 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases for the access point's Ethernet port, select the Ethertype name from the list box, then click **Delete**.

Step 2 Select one of the following:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining IP Protocol Filters

Procedure

Step 1 Select **Association > IP Protocol Filters.** The Association: IP Protocol Filters dialog box appears.

Step 2 With this option you can:

- Create new filters—See Creating New IP Protocol Filters, page 3-17.
- Delete the filters—See Deleting IP Protocol Filters, page 3-18.

Using this option you can also:

- Create Special Cases —See Creating Special Cases, page 3-18.
- Delete Special Cases—See Deleting Special Cases, page 3-21.

Creating New IP Protocol Filters

Procedure

Step 1 To create and enable IP protocol filters, enter the following:

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add.** The new name is added to the Current Protocol Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)

- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting IP Protocol Filters

Procedure

Step 1 To delete an IP protocol filter, select the name from the Current Protocol Filters list, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-5 IP Protocol Filters Special Cases Settings

Field	Description
Special Cases	
Protocol	Enter the IP protocol name.

Table 3-5 IP Protocol Filters Special Cases Settings (continued)

Field	Description
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the protocol filter. • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.

Table 3-5 IP Protocol Filters Special Cases Settings (continued)

Field	Description
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Click **Add.** The new name is added to the list box.

Step 4 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases, select the protocol name from the list box, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining IP Port Filters

Procedure

Step 1 Select **Association > IP Port Filters.** The Association: IP Port Filters dialog box appears.

Step 2 With this option you can:

- Create new filters—See Creating New Port Filters, page 3-22.
- Delete the filters—See Deleting Port Filters, page 3-23.

Using this option you can also:

- Create Special Cases —See Creating Special Cases, page 3-23.
- Delete Special Cases—See Deleting Special Cases, page 3-25.

Creating New Port Filters

Procedure

Step 1 To create and enable port filters, enter the following:

Field	Description
Add New Protocol Filter	
Set ID	Enter an identification number for the filter set.
Set Name	Enter a descriptive filter set name. See Naming Guidelines, page A-1.
Default Disposition	From the list, select one of the following: • Forward—Use this setting to forward traffic. • Block—Use this setting to block traffic.
Default Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the access point's buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the access point's buffer before they are discarded.

Step 2 Click **Add.** The new name is added to the Current Port Filters list.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Port Filters

Procedure

Step 1 To delete a protocol filter, select the name from the Current Port Filters list, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Creating Special Cases

Procedure

Step 1 Select the default filter for which you want to define a special case.

Step 2 Enter the following:

Table 3-6 IP Port Filters Special Cases Settings

Field	Description
Special Cases	
Port	Enter the IP Port filter name.
Disposition	From the list, select one of the following: • Default—Use the disposition you set for the port filter. • Forward—Use this setting to forward protocol traffic. • Block—Use this setting to block protocol traffic.

Table 3-6 IP Port Filters Special Cases Settings (continued)

Field	Description
Priority	From the list, select one of the following: • Default—This setting is the same as best effort, which applies to normal LAN traffic. • Background—Use this setting for bulk transfers and other activities that are allowed on the network but should not impact network use by other users and applications. • Excellent Effort—Use this setting for a network's most important users. • Controlled Load—Use this setting for important business applications that are subject to some form of admission control. • Interactive Video—Use this setting for traffic with less than 100 ms delay. • Interactive Voice—Use this setting for traffic with less than 10 ms delay. • Network Control—Use this setting for traffic that must get through to maintain and support the network infrastructure.
Time to Live (msec)	
unicast	Enter the number of milliseconds unicast packets should stay in the buffer before they are discarded.
multicast	Enter the number of milliseconds multicast packets should stay in the buffer before they are discarded.
Alert	From the list, select one of the following: • yes—Use this setting to send an alert to the event log when a user transmits or receives the protocol through the access point. • no—Use this setting to not send an alert to the event log.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Deleting Special Cases

Procedure

Step 1 To delete special cases, select the port name from the list box, then click **Delete**.

Step 2 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining Advanced Associations

Use this option to control the total number of devices an access point can list in the Association Table and the amount of time the access point continues to track each device class when a device is inactive.

Procedure

Step 1 Select **Association** > **Advanced**. The Association: Advanced dialog box appears.

Step 2 To define advanced associations, enter the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-7 Advanced Association Settings

Field	Description
Alert Severity Level	From the list select one of the following: • systemFatal—Indicates an event that prevents operation of the port or device. • protocolFatal—Indicates an event that prevents operation of the port or device • portFatal—Indicates an event that prevents operation of the port or device • systemAlert—Indicates that you need to take action to correct the condition. • protocolAlert—Indicates that you need to take action to correct the condition. • portAlert—Indicates that you need to take action to correct the condition. • externalAlert—Indicates that you need to take action to correct the condition.

Table 3-7 Advanced Association Settings (continued)

Field	Description
	• systemWarning—Indicates that an error or failure may have occurred. • protocolWarning—Indicates that an error or failure may have occurred. • portWarning—Indicates that an error or failure may have occurred. • externalWarning—Indicates that an error or failure may have occurred. • systemInfo—Notification that some sort of event has occurred. • protocolInfo—Notification that some sort of event has ocurred. • portInfo—Notification that some sort of event has ocurred. • externalInfo—Notification that some sort of event has ocurred.
Max Bytes Stored Per Alert Packet	Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event.
Max Fwd Table Entries	From the list, select one of the following to designate the maximum number of devices that can appear in the Association Table: 1024, 2048, 4096, 8192, 16384, 32768, 65536.

Table 3-7 Advanced Association Settings (continued)

Field	Description
Enable Extended Stats in MIB	From the list, select one of the following: • Enable—Use this setting to enable the storage of detailed statistics in the device's memory. • Disable—Use this setting to disable the storage of detailed statistics in the device's memory. When you disable extended statistics you conserve memory, and the device can include more devices in the Association Table.
Enable PSPF	From the list, select one of the following: • Enable—Use this setting to enable Publicly Secure Packet Forwarding, which ensures that client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses. • Disable—Use this setting to disable Publicly Secure Packet Forwarding. Click **see detail** to see for which versions this setting is valid.

Table 3-7 Advanced Association Settings (continued)

Field	Description
Unknown Class Timeout	Enter the number of seconds the access point continues to track an inactive device depending on its class. A setting of zero tells the access point to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.
Multicast Addresses Timeout	
Infrastructure Hosts Timeout	
Client Stations Timeout	
Repeaters Timeout	
Access Points Timeout	
Across Bridge Hosts Timeout	
Non-Root Bridges Timeout	
Root Bridges Timeout	

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Port Assignments

When you assign specific ports, your network topology remains constant even when devices reboot.

Procedure

Step 1 Select **Association** > **Port Assignments**. The Association: Port Assignments dialog box appears.

Step 2 To define port assignments, enter the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
ifIndex	Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.
dot1dBasePort	Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.
AID	Lists the port's 802.11 radio drivers association identifier.
Station	Enter the MAC address of the device to which you want to assign the port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring the Ethernet Port

Use this option to configure the device's Ethernet port.

Procedure

Step 1 Select **Ethernet**. The menu expands and the Ethernet dialog box displays in the right pane.

Step 2 Select one of the following from the Ethernet menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See Identifying the Ethernet Port, page 3-31.
- Filters—See Setting Up Ethernet Filters, page 3-32.
- Advanced—See Defining the Ethernet Advanced Settings, page 3-34.

Identifying the Ethernet Port

Use this option to define basic identity information for the Ethernet port.

Procedure

Step 1 Select **Ethernet** > **Identification**. The Ethernet: Identification dialog box displays in the right pane.

Step 2 Enter the following information to identify the port:

Field	Description
Primary Port?	From the list, select one of the following: • yes—Sets the Ethernet port as the primary port. • no—Sets the radio port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Ethernet Filters

Use this option to define filters for the Ethernet port, the IP Protocol, and the IP Port.

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Ethernet** > **Filters**. The Ethernet: Filters dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association** > **Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association** > **Ethertype Filters**.
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association** > **IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association** > **IP Protocol Filters**.
IP Port	
Receive	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association** > **IP Port Filters**.
Transmit	Enter the ID of a defined IP port filter, or select one of the filters you created using **Association** > **IP Port Filters**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)

- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Ethernet Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

Step 1 Select **Ethernet** > **Advanced**. The Ethernet: Advanced dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-8 Ethernet Advanced Settings

Field	Description
Status	From the list, select one of the following: • up— Enables the Ethernet port for normal operation. • down—Disables the device's Ethernet port.
Packet Forwarding	From the list, select one of the following: • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.

Table 3-8 Ethernet Advanced Settings (continued)

Field	Description
Default Multicast Address Filter	From the list, select one of the following: • allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under **Association > Address Filters**. • disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under **Association > Address Filters**.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.
Default Unicast Address Filter	From the list, select one of the following: • allowed—The access point forwards all traffic except packets sent to MAC addresses that have been set as disallowed under **Association > Address Filters**. • disallowed—The access point discards all traffic except packets sent to the MAC addresses that have been set as allowed under **Association > Address Filters**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring the Radio

Use this option to configure the device's radio.

Procedure

Step 1 Select **Radio**. The menu expands and the Radio dialog box displays in the right pane.

Step 2 Select one of the following from the Radio menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Identification—See Identifying the Radio Port, page 3-36.
- Filters—See Setting Up Radio Filters, page 3-38.
- Hardware—See Defining the Radio Hardware Settings, page 3-39.
- Advanced—See Defining the Radio Advanced Settings, page 3-44.
- Searched Channels—See Defining the Radio Searched Channels Settings, page 3-49.

Identifying the Radio Port

Use this option to define basic identity information for the Ethernet port.

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Radio** > **Identification**. The Radio: Identification dialog box displays in the right pane.

Step 2 Enter the following information to identify the port:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Primary Port?	From the list, select one of the following: • yes—Sets the radio port as the primary port. • no—Sets the Ethernet port as the primary port.
Adopt Primary Port Identity?	From the list, select one of the following: • yes—This adopts the primary port settings (MAC and IP addresses) for the Ethernet port. • no—This uses different MAC and IP addresses for the Ethernet port.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Up Radio Filters

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Radio > Filters**. The Radio Filters dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-9 Radio Filters Settings

Field	Description
Ethertype	
Receive	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
Transmit	Enter the ID of a defined Ethertype filter, or select one of the filters you created using **Association > Ethertype Filters**.
IP Protocol	
Receive	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.
Transmit	Enter the ID of a defined IP protocol filter, or select one of the filters you created using **Association > IP Protocol Filters**.

Table 3-9 Radio Filters Settings (continued)

Field	Description
IP Port	
Receive	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.
Transmit	Enter the ID of a defined IP port protocol filter, or select one of the filters you created using **Association > IP Port Filters**.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Radio Hardware Settings

Procedure

Step 1 Select **Radio > Hardware**. The Radio: Hardware dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-10 Radio Hardware Settings

Field	Description
Service SetID (SSID)	Enter a unique identifier client devices use to associate with the access point. It can be any alphanumeric, case-sensitive string, from 2 to 32 characters long. Several access points on a network or sub-network can share an SSID.
Allow "Broadcast" SSID to Associate	From the list, select one of the following: • yes—Allows devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) to associate with the access point. • no—Does not allow devices that do not specify an SSID (devices that are "broadcasting" in search of an access point to associate with) to associate with the access point. With no selected, the SSID used by the client device must match exactly the access point's SSID.
Enable "World Mode" multi-domain operation?	From the list, select one of the following: • yes—Allows the access point to add channel carrier set information to its beacon. Client devices with world-mode enabled receive the carrier set information and adjust their settings automatically. • no—Does not allow the access point to add channel carrier set information to its beacon.

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Data Rates (Mb/sec)	
1.0	From the list, select one of the following for each of the four rates in megabits per second: • basic—Allows transmission at this rate for all packets, both unicast and multicast. At least one data rate must be set to basic. • yes—Allows transmission at this rate for unicast packets only. • no—Does not allow transmission at this rate.
2.0	
5.5	
11.0	
Transmit Power	From the list, select one of the following milliwatt settings: 1, 5, 20, 30, 50, 100. To reduce interference or to conserve power, select a lower power setting.
Fragmentation Threshold (256-2338)	Enter a setting to determine the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.
RTS Threshold (0-2339)	Enter a setting to determine the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other.

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Maximum RTS Retries (1-128)	Enter the maximum number of times the access point issues an RTS before stopping the attempt to send the packet through the radio.
Max. Data Retires (1-128)	Enter the maximum number of attempts the access point makes to send a packet before giving up and dropping the packet.
Beacon Period (Kusec)	Enter the amount of time between beacons in Kilo microseconds. (One Kmsec equals 1,024 microseconds.)
Data Beacon Rate (DTIM)	Enter the amount of time, always a multiple of the beacon period, to determine how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them. If the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kmsecs. (One Kmsec equals 1,024 microseconds.)
Default Radio Channel	From the list, select the radio channel you want for a default. Each channel covers 22 MHz. The factory setting for Cisco wireless LAN systems is Radio Channel 6 transmitting at 2437 MHz.

Table 3-10 Radio Hardware Settings (continued)

Field	Description
Search for less-congested Radio Channel?	From the list, select one of the following: • yes—Allows the access point to scan for the radio channel that is least busy and selects that channel for use. • no—Will not allow the access point to scan for a radio channel that is least busy.
Receive Antenna Transmit Antenna	From the list, select one of the following: • Right—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's right connector. (When you look at the access point's back panel, the right antenna is on the right.) Use this setting for both receive and transmit. • Left—Use this setting if your access point has removable antennas and you install a high-gain antenna on the access point's left connector. (When you look at the access point's back panel, the left antenna is on the left.) Use this setting for both receive and transmit. • Diversity—Use this setting if your access point has two fixed (non-removable) antennas; it tells the access point to use the antenna that receives the best signal. Use this setting for both receive and transmit.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Radio Advanced Settings

Use this option to define the settings and operational status of the Ethernet port.

Procedure

Step 1 Select **Radio > Advanced**. The Radio: Advanced dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-11 Radio Advanced Settings

Field	Description
Status	From the list, select one of the following: • up— Enables the Radio port for normal operation. • down—Disables the device's Radio port.
Packet Forwarding	From the list, select one of the following: • enabled—Allows normal operation. • disabled—Prevents data from moving between the Ethernet and the radio, which is useful in troubleshooting.
Default Multicast Address Filter	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed under **Association > Address Filters**. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed under **Association > Address Filters**.
Maximum Multicast Packets/Second	Use this setting to control the number of multicast packets that can pass through the Ethernet port each second. If you enter 0, the access point passes an unlimited number of multicast packets. If you enter a number other than 0, the device passes only that number of multicast packets per second.

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Maximum Number of Associations	Enter the maximum number of wireless networking devices that are allowed to associate to the access point. If you enter 0 it means that the maximum possible number of associations is allowed. Click **see details** to see for which versions this setting is valid.
Use Aironet Extensions	From the list, select one of the following: • yes—Enable load balancing, Message Integrity Check (MIC), and WEP key hashing. • no—Does no enable the features listed above.
Ethernet encapsulation transform	From the list, select one of the following: • 802.1H—Provides optimum performance for Cisco Aironet wireless products. • RFC1042—Ensures interoperability with non-Cisco Aironet wireless equipment.
Enhanced MIC verification for WEP	From the list, select one of the following: • None—Does not enable MIC. • NMH—Enables MIC (Message Integrity Check), a security feature that protects your WEP keys by preventing attacks on encrypted packets called bit-flip attacks. Click **see details** to see for which versions this setting is valid.

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Temporal Key Integrity Protocol	From the list, select the following: • None—Does not enable WEP key hashing. • Cisco— Enables WEP key hashing that defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. Click **see details** to see for which versions this setting is valid.
Broadcast WEP Key rotation interval (sec)	Enter a rotation interval in seconds. • If you enter 900, for example, the access point sends a new broadcast WEP key to all associated client devices every 15 minutes. • If you enter 0, you disable broadcast WEP key rotation. Click **see details** to see for which versions this setting is valid.

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Default Unicast Address Filter	
Open	From the list, select one of the following: • Allowed—The access point forwards all traffic except packets sent to the MAC addresses set as disallowed with the Address Filters. • Disallowed—The access point discards all traffic except packets sent to the MAC addresses set as allowed with the Address Filters or on your authentication server. Select Disallowed for each authentication type that also uses MAC-based authentication.
Shared	
Network-EAP	
Specified Access Point 1	If this access point is a repeater, enter the MAC address of one or more root-unit access points with which you want this access point to associate. With MAC addresses in these fields, the repeater access point always tries to associate with the specified access points instead of with other less-efficient access points.
Specified Access Point 2	
Specified Access Point 3	
Specified Access Point 4	

Table 3-11 Radio Advanced Settings (continued)

Field	Description
Radio Modulation	From the list, select one of the following: • Standard—This setting is the modulation type specified in IEEE 802.11, the wireless standard published by the Institute of Electrical and Electronics Engineers (IEEE) Standards Association. • MOK—This modulation was used before the IEEE finished the high-speed 802.11 standard and may still be in use in older wireless networks.
Radio Preamble	From the list, select one of the following: • Long—Ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). • Short— Cisco Aironet's Wireless LAN Adapter supports short preambles; it improves throughput performance.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Radio Searched Channels Settings

Use this option to limit the channels that the access point scans when Search for less-congested radio channel is enabled.

The access point uses this setting to scan for the radio channel that is least busy and selects that channel for use.

Procedure

Step 1 Select **Radio** > **Searched Channels**. The Radio: Searched Channels dialog box displays in the right pane.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Channel Number	List the available channels by number.
Frequency (mHz)	Lists the channel frequency.
Search?	From the list, select one of the following: • Yes—Use this option to include the channel in the scan for less-congested channels. • No—Use this option to exclude the channel in the scan for less-congested channels

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Defining the Security Settings

Use this option to configure the device's security settings.

Procedure

Step 1 Select **Security**. The menu expands and the Security dialog box displays in the right pane.

Step 2 Select one of the following from the Security menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Local Admin Access—See Setting Local Admin Access, page 3-51.
- Local AP/Client Security—See Setting Local AP/Client Security, page 3-52.
- Server-Based Security—See Setting Server-Based Security, page 3-55.

Setting Local Admin Access

Use this option to enable or disable local admin access.

Procedure

Step 1 Select **Security > Local Admin Access**. The Security: Local Admin Access dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Local Admin Authentication	Select **Enable** to enable local admin authentication, or **Disable** to disable it.
Allow read-only browsing without login	Select **Yes** to allow it, or **No** to disallow it.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Local AP/Client Security

Use this option to set up the local access point and client security.

Procedure

Step 1 Select **Security > Local AP/Client Security.** The Security: Local AP/Client Security dialog box appears:

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-12 Local AP /Client Security Settings

Field	Description
Data Encryption by Stations	From the list, select the encryption type: • No Encryption—Requires clients to communicate with the Access Point without any data encryption. This setting is not recommended. • Optional—Allows clients to communicate with the Access Point either with or without data encryption. Typically, this option is used when you have client devices that cannot make a WEP connection, such as non-Cisco clients in a 128-bit WEP environment. • Full Encryption—Requires clients to use data encryption when communicating with the Access Point. Clients not using data encryption are allowed to communicate. This option is recommended if you want to maximize the security of your Wireless LAN.
Authentication Type	
Open	From the list, select one of the following: • Yes—Allows any device, regardless of its WEP keys, to authenticate and attempt to associate. This is the recommended setting. • No—Does not allow any device, regardless of its WEP keys, to authenticate and attempt to associate.
Shared Key	From the list, select one of the following: • Yes—Tells the access point to send a plain-text, shared key query to any device attempting to associate with the access point. This query can leave the access point open to a known-text attack from intruders. This is not as secure as the Open setting. • No—Does not allow the access point to send a plain-text, shared key query to any device attempting to associate with the access point.

Table 3-12 Local AP /Client Security Settings (continued)

Field	Description
Network-EAP	From the list, select one of the following: • Yes—Allows EAP-enabled client devices to authenticate through the access point. • No—Does not allow EAP-enabled client devices to authenticate through the access point.
Require EAP	
Open	From the list, select one of the following: • Yes—Use this option if you use open and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use open and EAP authentication.
Shared	From the list, select one of the following: • Yes—Use this option if you use shared and EAP authentication to block client devices that are not using EAP from authenticating through the access point. • No—Use this option if you do not use shared and EAP authentication.
Encryption Keys 1 through 4	
Transmit Key	Click to indicate this is the key you want to use to transmit packets. Only one key can be selected at a time.

Table 3-12 Local AP /Client Security Settings (continued)

Field	Description
Encryption Key	Enter the type of encryption key used: • For 40-bit WEP keys, enter as 10 hexadecimal digits (0-9, a-f, or A-F). • For128-bit WEP keys, enter as 26 hexadecimal digits (0-9, a-f, or A-F).
Key Size	From the list, select one of the following: • Not set • 40 bit • 128 bit

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Setting Server-Based Security

Use this option to set up server-based security.

Note Changing this setting may cause the access point to reboot.

Procedure

Step 1 Select **Security > Server-Based Security.** The Security: Server-Based dialog box appears:

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-13 Server-Based Security Settings

Field	Description
Server Name/IP	Enter the name or IP address of the server.
Server Type	Enter the type of server.
Port	Enter the port number your server uses for authentication.
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Time Out (sec's)	Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next defined authentication server.
Use this server for	

Table 3-13 Server-Based Security Settings (continued)

Field	Description
EAP Authentication	From the list, select one of the following: • Yes—Use this server for EAP authentication. In this type of authentication, the access point relays authentication messages between the server and the authenticating client device. • No—Do not use this server for EAP authentication. Click **see detail** to see for which versions this setting is valid.

Table 3-13 Server-Based Security Settings (continued)

Field	Description
MAC Address Authentication	From the list, select one of the following: • Yes—Use this server for MAC-based authentication. This allows only client devices with specified MAC addresses to associate and pass data through the access point. Client devices with MAC addresses not in a list of allowed MAC addresses are not allowed to associate with the access point. • No—Do not use this server for MAC-based authentication. Click **see detail** to see for which versions this setting is valid.

Table 3-13 Server-Based Security Settings (continued)

Field	Description
802.1X Protocol Version (For EAP Authentication)	From the list, select one of the following: • Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting. • Draft 8—Select this option if LEAP-enabled client devices that associate with this access point use radio firmware versions 4.13, 4.16, or 4.23, or if workgroup bridges associating with this access point use firmware version 8.58 or earlier. • Draft 10—Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication, if LEAP-enabled client devices that associate with this bridge use radio firmware version 4.25 or later, or if workgroup bridges associating with this access point use firmware version 8.65 or later. This is the default setting in access point and bridge firmware versions 11.06 and later.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Services

Use this option to configure various system features and support services on the device.

Procedure

Step 1 Select **Services**. The menu expands and the Services dialog box displays in the right pane.

Step 2 Select one of the following from the Services menu:

- Start-Up—See Configuring Start-Up Settings, page 3-61.
- Console/Telnet—See Configuring Console/Telnet Settings, page 3-63.
- Hot Standby—See Configuring Hot Standby Settings, page 3-65.
- Routing—See Configuring Routing Settings, page 3-67.
- CDP—See Configuring CDP Settings, page 3-68.
- DNS—See Configuring DNS Settings, page 3-69.
- FTP—See Configuring FTP Settings, page 3-70.
- HTTP—See Configuring HTTP Settings, page 3-72.
- SNMP—See Configuring SNMP Settings, page 3-73.
- SNTP—See Configuring SNTP Settings, page 3-74.
- Accounting—See Configuring Accounting Settings, page 3-75.

Configuring Start-Up Settings

Use this option to configure the access point for your network's BOOTP or DHCP servers for automatic assignment of IP addresses.

Procedure

Step 1 Select **Services** > **Start-Up.** The Services: Start-Up dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-14 Services Start-Up Settings

Field	Description
Configuration Server Protocol	From the list, select one of the following: • None—Use this setting if your network does not have an automatic system for IP address assignment. • BOOTP—Use this setting if IP addresses are hard-coded based on MAC addresses. • DHCP—Use this setting if IP addresses are "leased" for predetermined periods of time.
Use prior Config Server settings if no server responds?	From the list, select one of the following: • yes— Use this setting to have the access point save the boot server's most recent response. • no—Use this setting to not use the most recent response.

Table 3-14 Services Start-Up Settings (continued)

Field	Description
Read ".ini" file from file server?	From the list, select one of the following: • always—Use this setting for the access point to always load configuration settings from an .ini file on the server. • never—Use this setting for the access point to never load configuration settings from an .ini file on the server. • if specified by server—Use this setting for the access point to load configuration settings from an .ini file on the server if the server's DHCP or BOOTP response specifies that an .ini file is available.
BOOTP Server Timeout (sec's)	Enter the length of time the access point waits to receive a response from a single BOOTP server.
DHCP Multiple-Offer Timeout (sec's)	Enter the length of time the access point waits to receive a response when there are multiple DHCP servers.
DHCP Requested Lease Duration (min's)	Enter the length of time the access point requests for an IP address lease from your DHCP server.
DHCP Minimum Lease Duration (min's)	Enter the shortest amount of time the access point accepts for an IP address lease. The access point ignores leases shorter than this period.
DHCP Class Identifier	Enter the access point's group name. The DHCP server uses the group name to determine the response to send to the access point.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Console/Telnet Settings

Use this option to configure the access point to work with a terminal emulator or through Telnet.

Procedure

Step 1 Select **Services** > **Console/Telnet.** The Services: Console/Telnet dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-15 Services > Console/Telnet Settings

Field	Description
Baud Rate	Enter a rate from 110 to 115,200, expressed in bits per second. The rate you enter is dependent on the capability of the computer you use to open the access point management system.
Parity	From the list, select one of the following: • None—Use this setting to use no parity bit. • Even—Use this setting to make the total number of bits even. • Odd—Use this setting to make the total number of bits odd.
Data Bits	From the list, select one of the data bit settings.
Stop Bits	From the list, select one of the stop bit settings.
Flow Control	From the list, select one of the following: • None—Use this setting to indicate no flow control is used. • SW Xonn/Xoff—Use this setting to indicate the method information is sent between pieces of equipment to prevent loss of data when too much information arrives at the same time on one device.
Terminal Type	From the list, select one of the following: • teletype—Use this setting if your terminal emulator does not support ANSI. • ANSI—Use this setting to offer graphic features such as reverse video buttons and underlined links.

Table 3-15 Services > Console/Telnet Settings (continued)

Field	Description
Columns (64-132)	Enter a number to define the width of the terminal emulator display within the range of 64 characters to 132 characters.
Lines (16-50)	Enter a number to define the height of the terminal emulator display within the range of 16 characters to 50 characters.
Telnet	From the list, select one of the following: • Enable—Use this setting to enable Telnet access to the management system. • Disable—Use this setting to prevent Telnet access to the management system.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Hot Standby Settings

Use this option to configure a standby access point as a client device associated to a monitored access point.

Procedure

Step 1 Select **Services** > **Hot Standby**. The Services: Hot Standby dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Hot Standby Mode	From the list, select one of the following: • Enable—Use this setting to allow hot standby mode. • Disable—Use this setting to disable hot standby mode.
Service Set ID (SSID)	Enter the monitored access point's SSID.
MAC Address for the Monitored AP	Enter the monitored access point's MAC address.
Polling Frequency (1-30)	Enter the number of seconds between each query the standby access point sends to the monitored access point.
Timeout for Each Polling (1-600)	Enter the number of seconds the standby access point should wait for a response from the monitored access point before it assumes that the monitored access point has malfunctioned.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Routing Settings

Use this option to configure the access point to communicate with the IP network routing system.

Procedure

Step 1 Select **Services** > **Routing**. The Services: Routing dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Default Gateway	Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.
New Network Route	
Destination Network	Enter the IP address of the destination network.
Gateway	Enter the IP address of the gateway used to reach the destination network.
Subnet Mask	Enter the subnet mask associated with the destination network.

Step 3 Click **Add** to add an additional network route for the access point.

Step 4 To remove a network route, select it from the list, then click **Remove**.

Step 5 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring CDP Settings

Use this option to enable, disable, or adjust the access point's CDP settings.

Procedure

Step 1 Select **Services** > **CDP**. The Services: CDP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Cisco Discovery Protocol (CDP)	From the list, select one of the following: • Enable—Use this setting to enable CDP. • Disable—Use this setting to disable CDP.
Packet Hold Time	Enter the number of seconds other CDP-enabled devices should consider the access point's CDP information valid.
Packet Sent Every	Enter the number of seconds between each CDP packet the access point sends. This value should always be less than the packet hold time.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring DNS Settings

Use this option to configure the access point to work with your network's Domain Name System (DNS) server.

Procedure

Step 1 Select **Services** > **DNS**. The Services: DNS dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-16 Services > DNS Settings

Field	Description
Domain Name System (DNS)	From the list, select one of the following: • Enable—Use this option if your network DNS. • Disable—Use this option if you network does not use DNS.
Default Domain	Enter the name of your network's IP domain. Your entry might look like this: mycompany.com

Table 3-16 Services > DNS Settings (continued)

Field	Description
Domain Name Servers	Enter the IP addresses of up to three domain name servers on your network.
Domain Suffix	Enter the portion of the full domain name that you would like omitted from access point displays. For example, the full name of a computer might be "mycomputer.mycompany.com."If you set the domain suffix to "mycompany.com," the computer's name would be displayed as "mycomputer."

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring FTP Settings

Use this option to configure File Transfer Protocol settings for the access point. All non-browser file transfers are governed by these settings.

Procedure

Step 1 Select **Services** > **FTP**. The Services: FTP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-17 Services > FTP Settings

Field	Description
File Transfer Protocol (FTP)	From the list select one of the following: • TFTP • FTP
Default File Server	Enter the IP address or DNS name of the file server where the access point should look for FTP files.
FTP Directory	Enter the file server directory that contains the firmware image files.
FTP User Name	Enter the username assigned to your FTP server. You do not need to enter a name in this field if you selected TFTP.
FTP User Password	Enter the password associated with the file server's username. You do not need to enter a password in this field if you selected TFTP.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring HTTP Settings

Use this option to configure HTTP settings for the access point.

Procedure

Step 1 Select **Services** > **HTTP** The Services: HTTP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Allow Non-Console Browsing	From the list, select one of the following: • Enable—Use this setting to allow browsing to the management system. • Disable—Use this setting to make the management system accessible only through the console and Telnet interfaces.
HTTP Port	Enter the port through which the access point provides web access.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring SNMP Settings

Use this option to configure settings for notifications to be sent to an SNMP server.

Procedure

Step 1 Select **Services** > **SNMP**. The Services: SNMP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Simple Network Management Protocol (SNMP)	From the list, select one of the following: • Enable—Use this setting to allow event notifications to be sent to an SNMP server. • Disable—Use this setting to not allow event notifications to be sent to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring SNTP Settings

Use this option to configure time server settings.

Procedure

Step 1 Select **Services > SNTP**. The Services: SNTP dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Field	Description
Simple Network Time Protocol (SNTP)	From the list, select one of the following: • Enable—Use this setting if your network uses Simple Network Time Protocol. • Disable—Use this setting if your network does not use Simple Network Time Protocol.
Default Time Server	Enter enter the server's IP address.
GMT Offset (hr)	From the list, select the time zone in which the access point operates.
Use Daylight Savings Time	From the list, select one of the following: • Enable—Use this setting to have the access point automatically adjust to Daylight Savings Time. • Disable—Use this setting to not have the access point automatically adjust to Daylight Savings Time.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Accounting Settings

Use this option to configure settings that enable you to send network accounting information about wireless client devices to a RADIUS server on your network.

Procedure

Step 1 Select **Services** > **Accounting**. The Services: Accounting dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-18 Accounting Settings

Field	Description
Enable accounting	From the list, select one of the following: • enable—Use this setting to turn on accounting for your wireless network. • disable—Use this setting to turn off accounting for your wireless network
Enable delaying to report STOP	• enable—Use this setting to delay sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate. • disable—Use this setting to not delay sending a stop report to the server when a client device disassociates from the access point.
Minimum delay time to report STOP (sec)	Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point.
Server Name/IP	Enter the name or IP address of the server to which the access point sends accounting data.
Server Type	Select RADIUS from the list. (Additional types may be added in future software releases.)
Port	Enter the communication port setting used by the access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and Cisco secure ACS.

Table 3-18 Accounting Settings (continued)

Field	Description
Shared Secret	Enter the shared secret used by your server. It must match the shared secret on the RADIUS server.
Time Out (sec's)	Enter the number of seconds the access point should wait before authentication fails. If the server does not respond within this time, the access point tries to contact the next defined authentication server.
Enable Update	From the list, select one of the following: • enable—Use this setting to allow accounting update messages for wireless clients. With updates enabled, the access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. • disable—Use this setting to not allow accounting update messages. With updates disabled, the access point sends only accounting start and accounting stop messages to the server.
Update Delay (sec's)	Enter the update interval in seconds. If you use 360, the access point sends an accounting update message for each associated client device every 6 minutes.

Table 3-18 Accounting Settings (continued)

Field	Description
Use this server for	
EAP Authentication	From the list, select one of the following: • Yes—Use this server for EAP authentication. In this type of authentication, the access point relays authentication messages between the server and the authenticating client device. • No—Do not use this server for EAP authentication.
non-EAP Authentication	From the list, select one of the following: • Yes—Use this server for non-EAP authentication. • No—Do not use this server for non-EAP authentication.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Events

This option enables to you to customize the display of access point events (alerts, warnings, and normal activity).

Procedure

Step 1 Select **Events**. The menu expands and the Events dialog box displays in the right pane.

Step 2 Select one of the following from the Events menu:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

- Event Handling—See Configuring Event Handling, page 3-79.
- Event Notifications—See Configuring Event Notification, page 3-84.

Configuring Event Handling

The event settings control how events are handled by the access point: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information.

Procedure

Step 1 Select **Events** > **Event Handling**. The Events: Event Handling dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-19 Event Handling Settings

Field	Description
System Fatal	From the list, select one of the following: • Count—Use this option to tally the total events occurring in this category without any form of notification or display. • Display Console—Use this option to provide a read-only display of the event but not record it. • Record—Use this option to make a record of the event in the log and provide a read-only display of the event. • Notify—Use this option to makes a record of the event in the log, display the event, and tell the access point to notify someone of the occurrence.
Protocol Fatal	
Network Port Fatal	
System Alert	
Protocol Alert	
Network Port Alert	
External Alert	
System Warning	
Protocol Warning	
Network Port Warning	
External Warning	
System Information	
Protocol Information	
Network Port Information	
External Information	

Table 3-19 Event Handling Settings (continued)

Field	Description
Handle Alerts as Severity Level	From the list, select one of the following: • systemFatal—Indicates an event that prevents operation of the device as a whole. • protocolFatal—Indicates an event that prevents operation of a specific communications protocol in use, such as HTTP or IP. • portFatal—Indicates an event that prevents operation of the Ethernet or radio network interface. • systemAlert—Indicates that you need to take action to correct a condition on the device as a whole. • protocolAlert—Indicates that you need to take action to correct a condition on a specific communications protocol in use, such as HTTP or IP. • portAlert—Indicates that you need to take action to correct the condition on the Ethernet or radio network interface. • externalAlert—Indicates that you need to take action to correct the condition on a device on the network.

Table 3-19 Event Handling Settings (continued)

Field	Description
	• systemWarning—Indicates that an error or failure may have occurred on the device as a whole. • protocolWarning—Indicates that an error or failure may have occurred on a specific communications protocol in use, such as HTTP or IP. • portWarning—Indicates that an error or failure may have occurred on an Ethernet or radio network interface. • externalWarning—Indicates that an error or failure may have occurred on a device. • systemInfo—Notification that some sort of event has occurred on a device. • protocolInfo—Notification that some sort of event has ocurred on a communications protocol in use, such as HTTP or IP. • portInfo—Notification that some sort of event has ocurred on an Ethernet or radio network interface. • externalInfo—Notification that some sort of event has ocurred on a device.

Table 3-19 Event Handling Settings (continued)

Field	Description
Maximum Number of Bytes Stored per Alert Packet (0- 2312)	Enter the maximum number of bytes the access point stores for each Station Alert packet when packet tracing is enabled. If you use 0, the access point does not store bytes for Station Alert packets; it only logs the event. **Note** Changing this setting may cause the access point to reboot.
Maximum Memory Reserved for Detailed Event Trace Buffer (bytes) (0-8388608)	Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network. **Note** Changing this setting may cause the access point to reboot.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Event Notification

Use this option to enable and configure notification of fatal, alert, warning, and information events to destinations external to the access point, such as an SNMP server or a Syslog system.

Procedure

Step 1 Select **Events > Event Notification**. The Events: Event Notification dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Table 3-20 Events > Event Notification Settings

Field	Description
Should Notify-Disposition Events generate SNMP Traps?	From the list, select one of the of the following: • Yes—Use this option to send event notifications to an SNMP server. • No—Use this option if you do not want to send notifications to an SNMP server.
SNMP Trap Destination	Enter the IP address or the host name of the server running the SNMP Management software.
SNMP Trap Community	Enter the SNMP community name.
Should Notify-Disposition Events generate Syslog Messages?	From the list, select one of the of the following: • Yes—Use this option to send event notifications to a Syslog server. • No—Use this option if you do not want to send notifications to a Syslog server.

Table 3-20 Events > Event Notification Settings (continued)

Field	Description
Syslog Destination Address	Enter the IP address or the host name of the server running Syslog.
Syslog Facility Number	Enter the Syslog Facility number for the notifications.

Step 3 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Configuring Custom Values

This option enables to you to enter custom values that might not be available in the Template Menu. It also allows you to quickly enter a value, if you know the exact value you want to change, instead of going through the menu. (See Examples, page 3-86.)

Note This option should be used only by advanced users who have a good understanding of the MIB variables they are setting.

Templates with custom key values are not validated.

Procedure

Step 1 Select **Configure** > **Templates** > **Custom Values**. The Custom Values dialog box appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Template windows up until that point.

Step 2 Complete the following:

Note You must enter the exact syntax for the setting to work properly.

Field	Description
Key	Enter a valid MIB key. (See Examples, page 3-86.)
Value	Enter a valid MIB value. (See Examples, page 3-86.)

Step 3 Click **Add** to add the custom value to the list.

Note If the custom value you enter is the same as an existing one in the Template Menu, the custom value will override the value in the menu.

Step 4 To remove a custom value, select it from the list, then click **Remove**.

Step 5 Select one of the following in the left pane:

- **Preview** to see your changes before you apply them. (See Previewing the Template, page 3-89.)
- **Finish** to save the template. (See Finishing the Template, page 3-89.)
- Another template category to configure more options. (See Template Categories, page 3-2.)

Examples

Following are examples of custom key values that can be entered:

- Set system contact on access points.

  - **Key**: sysContact.0
  - **Value:** ABC, XYZ Inc.
- Set system location for access points.
  - **Key**:sysLocation.0
  - **Value:** Bldg ABC, XYZ Inc.
- Set up a user for an access point
  - **Key**:userMgrUserName.x
  - **Value:** testUser
  - **Key**:userMgrPassword.x
  - **Value:** testPassword
  - **Key**:userMgrCapabilities.x
  - **Value:** 20

  where:

  - x is the next available index in the user manager table (userMgrConfig Table)
  - Capabilities are the sum of any of the following: 0=none; 1=Administrator; 2=Write; 4=Firmware Update; 8=Identity Update; 16=SNMP Community
- Reboot an access point.
  - **Key**:tsMsgSend0
  - **Value:** 2

- Classify workgroup bridges as network infrastructure
  - **Key**:awcDot11DesiredSSIDInfrastructureWGB.2
  - **Value:** false

  where the possible values are T (true) and F (false)
- Set the DHCP Client Identifier Type
  - **Key**:bootconfigDhcpClientIdType
  - **Value:** ethernet10Mb

  where the possible values are text or numeric:
  - ethernet10Mb or 1
  - experimentalEthernet3Mb or 3
  - amateurRadioAxDot25 or 3proteonProNetTokenRing or 4
  - chaos or 5
  - ieee802Networks or 6
  - arcnet or 7
  - hyperchannel or 8
  - lanstar or 9
  - autonet or 10
  - localTalk or 11
  - localNet or 12
  - nonHardware or 128
- Set the DHCP client Identifier Value
  - **Key:** bootconfigDhcpClientIdValue
  - **Value:** 22

- Is MAC alone sufficient for to be fully authenticated
  - **Key:** awcFtEnableMacOrEapAuth
  - **Value:** F

  where the possible values are T (true) and F (false)
- Set Rogue AP alert timeout (minutes)
  - **Key:** awcFtRogueApAlertTimeout
  - **Value:** 29
- Use symbol extensions
  - **Key:** awcDot11SymbolExtensionsEnabled.2
  - **Value:** 2

  where the possible values are T (true) and F (false)

Previewing the Template

Procedure

Step 1 Click **Preview.** A window displays the configuration choices you have made to the template.

Step 2 Click Finish. (See Finishing the Template, page 3-89.)

Finishing the Template

Procedure

Step 1 Click **Finish** in the left pane to complete creating a template. The Finish dialog box appears in the right pane.

Note It is recommended that you always validate the template before saving it.

Step 2 Click **Validate** if you want to check the template configuration. A window displays a message indicating for which devices and versions the configuration template you just created is valid.

Note Templates containing custom key values are not validated.

Step 3 Check **Enable Version Check** if you want the system to make sure you apply the templates only to devices with valid versions.

If you do not enable the version check, templates will be applied to devices even when the configuration is not valid for the device version.

Step 4 Click **Save** to create the template. The screen refreshes and the template name appears in the Existing Templates listbox.

Creating a Template

Use this option to create a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure > Templates**. The Templates dialog box appears.

Step 2 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 3 Click **Create New**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.

Step 4 Select the choices in the left pane to create a configuration template. For a description, see Template Choices, page 3-2.

Copying a Template

Use this option to copy a configuration template that you can use as a base for another template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select the template you want to copy from the Existing Templates box, then click **Create Copy**. A dialog box appears asking you to enter a name for the copy.

Step 3 Enter a unique name. (See Naming Guidelines, page A-1 for details.)

Step 4 Click **OK**. The Templates window refreshes and the new name appears in the Existing Templates list.

Step 5 Click **Edit.** (See Editing a Template, page 3-91.)

Editing a Template

Use this option to edit a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select the template you want to edit from the Existing Templates box, then click **Edit**. The window refreshes with Template Creation menu in the left pane and the Template Name dialog box in the right pane.

Step 3 Select the choices in the Template Menu to create a configuration template. For a description, see Template Choices, page 3-2.

Deleting a Template

Use this option to delete a configuration template.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Templates**. The Templates dialog box appears.

Step 2 Select the template you want to delete from the Existing Templates box, then click **Delete**. A window appears asking if you want to delete the template.

Step 3 Click **OK** to delete it.

Managing Configuration Jobs

This is window allows you view a list of all the jobs in their various states. It also allows you to create, edit, and filter, and undo configuration jobs.

The topics covered in this section are:

Related Topic

Using the Templates, page 3-1.

Job Choices

When you create or edit a configuration job, the following choices appear in the left pane of the Jobs window:

Note These are steps that must be completed but do not have to be done in order.

1. **Job Name**—See Naming the Job, page 3-93.
2. **Select Devices**—See Naming the Job, page 3-93.
3. **Select Template**—See Selecting a Template, page 3-95.
4. **Schedule Job**—See Scheduling a Job, page 3-97.

Caution Clicking on another tab before you have saved your entries in this window will cause the window to reset and you will lose all the information you entered.

Naming the Job

Procedure

Step 1 Click **Job Name.** The Job Name dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-21 Job Name

Field	Description
Job Name	Enter a name for the job. See Naming Guidelines, page A-1.
Description	Enter a description of the job. See Naming Guidelines, page A-1.
Protocol	Select the type of protocol used: HTTP or SNMP. **Note** If you select SNMP, you will not be able to use the Undo feature; it is only supported for HTTP-based configuration jobs.

Step 3 From the menu in the left pane, go to the next step, Select Devices. (For additional information, see Selecting Devices, page 3-94.)

Selecting Devices

Procedure

Step 1 Click **Select Devices.** The Select window appears.

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Step 2 From the device selector, click the folder from which you want to build a device list.

Clicking the folder displays the folder's contents in the All Available Devices list box.

Repeat this step as many times as necessary to select devices from the folder in which they reside.

Step 3 From the All Available Devices list, select folders or individual devices, then click **Add**. The devices appear in the Selected Devices list box.

Note If you select a folder, the template will be applied to all of the devices in that folder. If a device is subsequently added to the folder, the template is applied to that device.

Step 4 To remove devices, select them from the Devices in Group list, then click **Remove**.

Step 5 From the menu in the left pane, go to the next step, Select Template. (For additional information, see Selecting a Template, page 3-95.)

Selecting a Template

Procedure

Step 1 Click **Select Template.** The Select Template window appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-22 Select Template

Field	Description
Configuration Template	From the list, select the template which you want to apply to the devices.
Details	
Name	Displays the name of the selected template.
Device Types	Displays the device types that are valid for the selected template.
Device Versions	Displays the device versions for the device types listed in the Device Type field. Each device type's valid versions are displayed in sequence and grouped using parentheses.
Description	Displays the template description.
Version Check Enabled	Indicates whether the version check is enabled. (The check is enabled using the Finish step in the Template Menu.)

Step 3 From the menu in the left pane, go to the next step, Schedule Job. (For additional information, see Scheduling a Job, page 3-97.)

Scheduling a Job

Procedure

Step 1 Click **Schedule Job.** The Schedule Job dialog box appears.

Step 2 Complete the following:

Note Clicking **Clear** removes all the current entries in the window and any entries you have made in other Job windows up until that point.

Table 3-23 Schedule Job

Field	Description
Run Now	Click to run the job. (The job begins running in 2 minutes.) **Note** This option ignores any dates you have entered in Start Date and Start Time.
Start Date	From the lists, select the month, day, and year you want your job to run.
Start Time	From the list, select the hour and minutes of the day you want your job to run.
Repeat	
Enable	Check to run the job repeatedly.
Every	Indicate how often you want the job to repeat by entering a numerical value, then selecting an interval of time: Hours, Days, Months, or Years.

Step 3 From the menu in the left pane, go to the next step, Finish. (For additional information, see Finishing Scheduling, page 3-98.)

Tip You can stop a running job by clicking **Stop Job**.

Finishing Scheduling

Procedure

Step 1 Click **Finish** in the left pane to complete creating a job. The Finish dialog box appears in the right pane.

Step 2 Do one of the following:

Note It is recommended that you always validate the job before saving it.

- Click **Validate** if you want to check the job.

  A window displays a confirmation message if the job is successful, and an informational message if the selected template in the job is not valid for the selected devices.

Note Jobs with templates containing custom key values are not validated.

- Click **Save** to create the job. The screen refreshes and
  - The job name appears in the Scheduled Jobs list.
  - A confirmation window appears with the job summary.

Creating a Configuration Job

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Configure** > **Jobs**. The Jobs window appears.

Step 2 Enter a name for the job. See Naming Guidelines, page A-1.

Step 3 Click **Create Job.** The window refreshes with Job Creation menu in the left pane and the Job Name dialog box in the right pane.

Step 4 Select the numbered choices in the left pane to create a job. For a description, see Job Choices, page 3-93.

Viewing Configuration Job Status

This is window allows you to view job status. It also allows you to filter a job, edit a job, view details about the job and undo a job.

Device data is polled is every 15 minutes by default, and the duration that job data is retained is 30 days. To change either default, see Managing System Parameters, page 5-58.

The topics covered in this section are:

- Viewing the Job State, page 3-100
- Filtering a Job, page 3-102
- Editing a Job, page 3-102
- Deleting a Job, page 3-103
- Stopping a Job, page 3-103
- Viewing Job Run Details, page 3-103

Note Your login determines whether you can use this option.

Related Topic

Using the Templates, page 3-1

Viewing the Job State

Procedure

Step 1 From the Job State list, select the type of job whose status you want to check. The window refreshes and the jobs are displayed.

The tables vary depending on which type of Job State you selected: Scheduled and Unscheduled, Running, or All:

- Scheduled and Unscheduled

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the last run.

- Running

Tip You can stop a running job by clicking **Stop Job**.

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job Start Time	The time the job started.

Field	Description
Percent Complete	The percent of the job that has completed running.
Next Schedule	The next time the job is scheduled to run.

- All

Field	Description
Job Name	The job name.
Recurring	Whether the job recurs.
Job State	The state of the job. **Note** A job in a DidNotStart state must be rescheduled.
Next Schedule	For scheduled jobs, this indicates the next time the job will run. For completed jobs, this is last time the job ran.
Last Run Status	The status of the job the last time it run.

Step 2 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 3 You can do any of the following:

a. Filter the job—See Filtering a Job, page 3-102.

b. Edit the job—See Editing a Job, page 3-102.

c. Delete the job—See Deleting a Job, page 3-103,

d. Stop a job—See Stopping a Job, page 3-103.

e. View the run details—See Viewing Job Run Details, page 3-103.

f. Refresh the screen—Click **Refresh**.

Filtering a Job

Use this option to filter jobs from the displayed list. Filtering this way allows you to display a limited set of jobs, making it easier to search for a particular job if you know the name.

Procedure

Step 1 Click **Filter Job.** The Filter Job dialog box appears.

Step 2 Enter the name, or part of the a name, on which to filter. (Use % as a wildcard to filter jobs. For example, entering %name% will filter all the jobs that contain "name.")

Step 3 Click **Apply filter.** The Job window refreshes and the matching jobs are displayed on the Jobs list.

Note The filter is only applied until the page is refreshed.

Editing a Job

Use this option to edit jobs from the displayed list of jobs.

Procedure

Step 1 Select the job from the list which you would like to edit.

Step 2 Click **Edit.** The Job Name dialog box appears.

Step 3 Select the choices in the Template Menu to create a configuration template. For a description, see Job Choices, page 3-93.

Deleting a Job

Use this option to delete jobs from the displayed list of jobs. Jobs that are scheduled, unscheduled, completed and did not start can be deleted. Jobs that are running cannot be deleted; they can be stopped.

Procedure

Step 1 Select the job from the list which you would like to edit.

Step 2 Click **Delete.**

Stopping a Job

Use this option to stop a job when it is in a running state.

Procedure

Step 1 Select the job from the list which you would like to stop.

Step 2 Click **Stop Job**. A window displays to confirm that you want to stop the job.

Step 3 Click **OK**, and the job stops.

Viewing Job Run Details

Use this option to view details about a job, or to undo a job from the displayed list of jobs.

Procedure

Step 1 From the All Jobs table displayed in **Configure > Jobs** window, select a job for which you would like to see details, then click **Job Run Detail**.

Step 2 The details window appears with the Job Runs table:

Field	Description
Select Run	Used to select a job for which you want to see more details.
Job Start Time	The time the job started.
Job End Time	The time the job ended.
Job Status	The status of the job.
Percent Complete	The percent of the job that completed.

Step 3 Do any of the following:

- To view details for a particular job run or to undo a job, select the job, then click **Show Run Details**. The Job Run details table displays the information. (See Viewing the Job Run Details Table, page 3-104.)
- To view the job run log, click **Job Run Log**. A window displays all the details for the selected job number.
- To refresh the table, click **Refresh**.

Viewing the Job Run Details Table

The Job Runs Details table displays the following information:

Field	Description
Device Name	The name of the device.
Start Time	The time the job started.
End Time	The time the job ended.
Status	The status of the job.

- To sort table data, click on the column heading by which you want to sort the data:
  - A triangle indicates ascending order.
  - An upside-down triangle indicates descending order.
  - No triangle indicates that the data is not sorted.
- To select all the jobs in the table, click **Select All.**
- To deselect all the jobs in the table, click **DeSelect All**.

Note If you have multiple screens, you must Select All or DeSelect All one screen at a time.

- To undo the selected configuration job, click **Undo**.

  The Undo feature is supported only for HTTP-based configuration jobs (not SNMP-based configurations jobs). It is not supported for:
  - Custom Values
  - Security options: Local Admin Authentication under the Local Admin Access; Encryption Key Values under Local AP/Client Security; Shared Secret under Server-Based Security; and Shared Secret under Accounting.
  - FTP username and password
  - Previously undone jobs

Using Reports

The Reports tab displays information about your devices. You can save and email reports. You can also set specific times for emailed reports to be run and sent automatically.

The reports available are dependent on the groups of devices and individual devices you choose from the selector in the left pane.

Following are the subtabs under Reports:

Note Some of the subtabs may not be visible to some users.

- **Wireless Clients**—See Displaying Wireless Client Reports, page 4-1
- **Current**—See Displaying Current Reports, page 4-6
- **Trends**—See Displaying Trends, page 4-21
- **Scheduled Email Jobs**—See Scheduling Email Jobs, page 4-29

Displaying Wireless Client Reports

Wireless client reports provide information about the type of client that is associating with an access point, information about how much bandwidth the client is using, and a history of which access points the client has been associated with.

Using this window, you can search for a wireless client based on their MAC address or name.

The frequency with which the Wireless Clients reports are updated is 5 minutes by default. To change the default setting, see Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option.

Following are the report types you can view:

- Client Detail Report—See Displaying a Client Detail Report, page 4-2
- Client Statistics Report—See Displaying a Client Statistics Report, page 4-3
- Client Historical Association Report—See Displaying a Client Historical Association Report, page 4-5

Displaying a Client Detail Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Note The MAC address must be entered in hexadecimal, for example 0070eb37c90.

Step 4 Click **Search**. A list appears in the left pane.

If you chose MAC address in the previous step, MAC addresses are listed; if you chose name, names are listed.

Step 5 Click the MAC address or name. The right pane refreshes and displays the Client Detail Report, which is the default report, with the following information:

Column	Description
Name	The name assigned to the wireless client device.
IP Address	The IP address of the wireless client device.
Classification	The type of wireless client device.
Associated with	The name or IP of the access point with which it was last associated.
State	The operational state of the wireless client device.
Time last seen	The time the client was last seen by the system.
Software Version	The version of wireless client software.
MAC Address	The MAC address of the wireless client.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Client Statistics Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Step 4 Click **Search**. A list appears in the left pane.

Step 5 Select the MAC address or name. The right pane refreshes.

Step 6 From the Report Name list, select Client Statistics Report.

Step 7 Click **View**. The Client Statistics Report displays in the right pane with the following information:

Table 4-1 Client Statistics Report

Column	Description
Name	The name of the wireless client.
IP address	The IP address of the wireless client.
Time last seen	The time the wireless client was last seen by the system.
Packets transmitted	The number of packets transmitted.
Octets transmitted	The number of octets transmitted.
Packets received	The number of packets received.
Octets received	The number of octets received.
Latest received signal strength	A tally of the received signal quality.
Latest signal quality	The current index of radio signal quality.
Sleep time in power save mode	The number of beacon intervals across which the station will sleep in power-save mode, or 1 if the station will never be in power-save mode.
Preferred transmission rate	The preferred data transmission rate.
Short retries	The number of times the RTS (request to send) packet had to be retried.
Latest short retries	A tally of the number of retries.
Long retries	The number of times the data packet had to be retried.
Latest long retries	A tally of the number of retries.
Received WEP errors	The number of received encryption errors.
Errors in transmitted packets	The number of errors in transmitted packets.
Errors in received packets	The number of errors in received packets.

Table 4-1 Client Statistics Report (continued)

Column	Description
Errors in received octets	The number of errors in received octets.
Announcements sent	The total number of announcement packets sent since the device was reset.

Step 8 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 9 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Client Historical Association Report

Procedure

Step 1 Select **Reports** > **Wireless Clients**. The Wireless Clients selector appears in the left pane.

Step 2 From the list, select the method you want to use to search for clients: by MAC address or name.

Step 3 Enter the MAC address or name. You can use an asterisk (*) as a wildcard to denote numbers and letters.

Step 4 Click **Search**. A list appears in the left pane.

Step 5 Select the MAC address or name. The right pane refreshes.

Step 6 From the Report Name list, select Client Historical Association Report.

Step 7 Click **View**. The Client Historical Association Report displays in the right pane with the following information:

Column	Description
Associated with	The name or IP address of the AP. Click on this link to view the AP Summary Report and the Fault Summary. For more information, see Displaying an AP Summary Report, page 4-11.
Client IP Address	The IP address of the AP.
Software Version	The software version of the wireless client device.
Time	The time the client was last seen by the system. For more information, see Date and Time Display on the WLSE, page 1-2.

Step 8 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 9 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 10 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying Current Reports

This window allows you to view current information about the monitored devices in your network. You can view, export, and email the reports.

The frequency with which configuration data is collected from the devices is 15 minutes by default. To change the default setting, see Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option.

Following are the report types you can view:

- Access Points and Bridges
  - Group Report—See Displaying a Group Report, page 4-7
  - Group Security Report—See Displaying a Group Security Report, page 4-9
  - Summary Report—See Displaying an AP Summary Report, page 4-11
  - Detailed Report—See Displaying a Detailed Report, page 4-13
  - Current Client Association—See Displaying a Current Client Association Report, page 4-15
  - EAP Authentication Report—See Displaying an EAP Authentication Report, page 4-16
- Switches
  - Switch Summary Report—See Displaying a Switch Summary Report, page 4-17
  - AP and Bridge Connected to Switch Report—See Displaying an AP and Bridge Connected to Switch Report, page 4-18
- Routers
  - Router Summary Report—Displaying a Router Summary Report, page 4-19
  - AP and Bridge Connected to Router Report—SeeDisplaying an AP and Bridge Connected to Router Report, page 4-20

Displaying a Group Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder for the group reports you want to view. The right pane refreshes.

Step 3 From the Report Name list, select Group Report.

Step 4 Click **View**. The group report is displayed with the following headings:

Column	Description
AP Name	The name of the access point. Click to view a detailed report. See Displaying a Detailed Report, page 4-13.
AP IP Address	The IP address of the access point. Click to open up a browser window to the AP Summary Status.
Number of Clients connected	The number of clients currently connected to the access point.
Number of Bridges connected	The number of bridges connected to the access point.
Number of AP-Repeaters Connected	The number of repeaters connected to the access point.
Number of Users Connected	The number of current users.
Status (Fault)	Click to view the Fault Summary. For more information, see Viewing Fault Details, page 2-6.
Timestamp	The time the access point's state last changed. For more information, see Date and Time Display on the WLSE, page 1-2.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Group Security Report

Procedure

Step 1 Select **Reports** > **Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder for the group security reports you want to view.

Step 3 From the Report Name list, select Group Security Report.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 4-2 Group Security Report

Column	Description
AP Name	The name of the device. Click to view the AP Detailed Report, Fault Summary, and the EAP Authentication Report. For more information, see Naming Guidelines, page A-1.
AP IP Address	The IP address of the device. Click to open up a browser window to the AP Summary Status.
Encryption type	Indicates the type of encryption used: No Encryption, Optional, or Full Encryption.
Length of WEP Key1 through 4 (in bits)	The WEP key length.

Table 4-2 Group Security Report (continued)

Column	Description
Authentication Type - Open System	Indicates whether any device, regardless of its WEP keys, can authenticate and attempt to associate.
Authentication Type - Shared Key	Indicates whether an access point sends a query to any device attempting to associate with the access point.
Status (Fault)	Click to view the Fault Summary. For more information, see Viewing Fault Details, page 2-6.
Link to EAP Authentication Report	Click to view the EAP Authentication report. For more information, see Displaying an EAP Authentication Report, page 4-16.
Timestamp	The time the fault was reported. For more information, see Date and Time Display on the WLSE, page 1-2.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP Summary Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder and select the device for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Summary Report**.

Step 4 Click **View**. Two tables are displayed: the AP Summary Report and the Fault Summary.

Table 4-3 AP Summary Report

Column	Description
Name	The system name for the device.
Timestamp	The time the fault was reported. For more information, see Date and Time Display on the WLSE, page 1-2.
MAC Address	The device's MAC address.
IP Address	The device's IP address. Click to open up a browser window to the AP Summary Status.
Software Version	The version of software running on the device.
Number of Clients connected	The number of wireless clients connected to the device.
Number of Bridges Connected	The number of wireless bridges connected to the device.
Number of AP-Repeaters Connected	The number of AP repeaters connected to the device.
Number of Users Connected	The number of users currently connected to the device.

Table 4-3 AP Summary Report (continued)

Column	Description
Model	Model number of the device.
Radio Service Set ID	The device's radio SSID.
Root or Repeater	Indicates whether the device is used as a root or repeater.
Link to the Detailed Report	Click to see details. For more information, see Displaying a Detailed Report, page 4-13.
Link to the Association Report	Click to see associations. For more information, see Displaying a Current Client Association Report, page 4-15.
Link to the Access Point Web Page	Click to open up a browser window to the AP Summary Status.

For information on the Fault Summary, see Viewing Fault Details, page 2-6.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Detailed Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder and select the device for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Detailed Report**.

Step 4 Click **View**. In addition to the Detailed Report, the Fault Summary, and the EAP Authentication Report are also displayed.

Table 4-4 Detailed Report

Column	Description
System Name	The system name for the device.
Timestamp	The time the device's state last changed. For more information, see Date and Time Display on the WLSE, page 1-2.
MAC Address	The device's MAC address.
IP Address	The device's IP address. Click to open up a browser window to the AP Summary Status.
Software Version	The device's software version.
Number of Clients connected	The number of clients connected to the device.
Number of Bridges Connected	The number of bridges connected to the device.
Number of AP-Repeaters Connected	The number of AP repeaters connected to the device.
Number of Users Connected	The number of users connected to the device.
Model	The hardware model of the device.
Radio Service Set ID	The device's SSID.

Table 4-4 Detailed Report (continued)

Column	Description
Root or Repeater	Indicates the role of the device.
Subnet Mask	The subnet mask.
Ensure Compatibility With 2Mbps Clients	Indicates whether it is compatible with 2Mbps clients.
Ensure Compatibility With non-Aironet 802.11	Indicates whether it is compatible with 802.11.
SNMP Trap Destination	The IP address or host name of the server running the SNMP Management software.
HTTP Port	The device's HTTP setting.
Hot StandBy	Indicates whether the hot standby unit is in monitoring mode. If true, the current unit is in monitoring mode.
Count of Access Point observed by this AP	Number of access points seen by the access points.
Current operating frequency channel	The radio channel being used.
Ethernet Port Status	The operational status of the Ethernet port.
Radio Port Status	The operational status of the radio port.
Transmit Power (mW)	The access point's transmission power setting in milliwatts.
Switch IP (to which this AP is attached)	The IP address of the switch to which this access point is attached.
Switch Name (to which this AP is attached)	The name of the switch to which this access point is attached.
Encryption type	Indicates that devices using WEP are allowed to communicate with the access point.
Length of WEP key 1 through 4 (in bits)	The WEP key length.

Table 4-4 Detailed Report (continued)

Column	Description
Authentication Type - Open System	Indicates whether any device, regardless of its WEP keys, can authenticate and attempt to associate.
Authentication Type - Shared Key	Indicates whether an access point sends a query to any device attempting to associate with the access point.
Link to the Access Point Web Page	Click to open up a browser window to the AP Summary Status.

- For Fault Summary information, see Viewing Fault Details, page 2-6.
- For EAP Authentication Report, see Displaying an EAP Authentication Report, page 4-16.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Current Client Association Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Current Client Association Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 4-5 Current Client Association Report

Column	Description
Name	The name of the client associated with the access point.
IP Address	The IP address of the wireless client.
MAC Address	The wireless client's MAC address.
Device Type	The wireless client device type.
Timestamp	The time the device was last seen by the system. For more information, see Date and Time Display on the WLSE, page 1-2.
State	The operational state of the device.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an EAP Authentication Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder and select the access point for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **EAP Authentication Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 4-6 EAP Authentication Report

Column	Description
Server Name	The name of the authentication server.
Server Protocol	The protocol used by the server.
Server Priority	The priority of the server when multiple servers are configured for the same service.
Server Port	The communication port setting used by the access point and the server.

Step 5 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Switch Summary Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the Switches folder and select the switch for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Switch Summary Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 4-7 Switch Summary Report

Column	Description
System Name	The switch name.
IP Address	The switch IP address or hostname.
Status (Fault)	The fault status. Click for details. For more information, see Viewing Fault Details, page 2-6.
System Description	A description of the switch.
Location	The location of the switch.
Product Type	The switch hardware type.
System Version	The switch version.
Link to the AP and Bridge Connected	Click for details. For more information, see Displaying an AP and Bridge Connected to Switch Report, page 4-18.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge Connected to Switch Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the Switches folder and select the switch for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge Connected to Switch Report**.

Step 4 Click **View**. The report is displayed with the following headings:

Table 4-8 AP and Bridge Connected to Switch Report

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the switch.
AP IP Address	The IP address of the access point or bridge connected to the switch.
Status (Fault)	The fault status. Click for details. For more information, see Viewing Fault Details, page 2-6.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Router Summary Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the Routers folder and select the router for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Router Summary Report**.

Step 4 Click **View**. The group report is displayed with the following headings:

Table 4-9 Router Summary Report

Column	Description
System Name	The router name.
IP Address	The router IP address.
Status (Fault)	The fault status.
System Description	A description of the router.
Location	The location of the router.
Product Type	The router hardware type.
System Version	The router version.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge Connected to Router Report

Procedure

Step 1 Select **Reports > Current**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the Routers folder and select the switch for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge Connected to Router Report**.

Step 4 Click **View**. The report is displayed with the following headings:

Column	Description
Device Port	The device port.
AP Name	The name of the access point or bridge connected to the router.
AP IP Address	The IP address of the access point or bridge connected to the router.
Status (Fault)	The fault status. Click for details. For more information, see Viewing Fault Details, page 2-6.

Step 5 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 6 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying Trends

This window allows you to view trends about the monitored devices in your network. You can view, export, and email the reports.

The frequency with which performance data is aggregated is 3 hours by default. To change the default setting, see Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option.

Following are the trend reports you can view for access points and bridges:

- Group Performance Report: RF Throughput—See Displaying a Group Performance Report: RF Utilization, page 4-22.
- Group Performance Report: Number of Associations—See Displaying a Group Performance Report: Ethernet Utilization, page 4-23.
- AP and Bridge RF Transmission Statistics—See Displaying an AP and Bridge RF Transmission Statistics, page 4-24.

- AP and Bridge Ethernet Transmission Statistics—See Displaying an AP and Bridge Ethernet Transmission Statistics, page 4-25.
- AP and Bridge Performance: Graph—See Displaying an AP and Bridge Performance: Graph, page 4-26.
- AP and Bridge Performance: Tabular—See Displaying an AP and Bridge Performance: Tabular, page 4-27.

Displaying a Group Performance Report: RF Utilization

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want a report. The right pane refreshes.

Step 3 From the Report Name list, select **Group Performance Report: RF Utilization.**

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. The table is displayed:

Column	Description
AP Name	The name of the access point.
IP Address	The IP address of the access point.
Timestamp	The start of the aggregate time period.
RF Utilization (%)	The percentage of radio frequency utilization.
Number of Associations	Shows the number of associations with clients.

Step 6 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 7 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 8 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying a Group Performance Report: Ethernet Utilization

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click the group folder for which you want to see a report. The right pane refreshes.

Step 3 From the Report Name list, select **Group Performance Report: Ethernet Utilization**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. The table is displayed:

Column	Description
AP Name	The name of the access point.
AP IP Address	The IP address of the access point.
Timestamp	The start of the aggregate time period.
Ethernet Utilization (%)	The percentage of Ethernet utilization.
Number of Associations	Shows the number of associations with clients.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge RF Transmission Statistics

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder, then select the devices for which you want to see a report. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge RF Transmission Statistics**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. A graph is displayed:

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.
Packet Errors	The x-axis displays the time intervals. The y-axis displays the number of error packets per number of packets.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge Ethernet Transmission Statistics

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder, then select the devices for which you want to see a report. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge Ethernet Transmission Statistics**.

Step 4 From the Start Date and End Date lists, select the start date and end date for the period of time for which you want trending information.

Step 5 Click **View**. A graph is displayed:

Column	Description
Transmit Rate	The x-axis displays the time intervals. The y-axis displays the number of packets transmitted per second.
Receive Rate	The x-axis displays the time intervals. The y-axis displays the number of packets received per second.
Packet Errors	The x-axis displays the time intervals. The y-axis displays the number of error packets per number of packets.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge Performance: Graph

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge Performance Graph**.

Step 4 From the Start Date list, select the start date for the graph, an d from the For a period of list, select the number of days.

Step 5 Click **View**. A graph is displayed:

Column	Description
Number of Associations	The x-axis displays the time intervals. The y-axis displays the number of client associations
RF Utilization	The x-axis displays the time intervals. The y-axis displays the percent of radio frequency utilization.
Ethernet Utilization	The x-axis displays the time intervals. The y-axis displays the percent of Ethernet utilization.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Displaying an AP and Bridge Performance: Tabular

Procedure

Step 1 Select **Reports** > **Trends**. The window refreshes with a device selector in the left pane.

Step 2 From the device selector in the left pane, click to expand the folder you want to view. The right pane refreshes.

Step 3 From the Report Name list, select **AP and Bridge Performance: Tabular**.

Step 4 From the Start Date list, select the start date for the graph, an d from the For a period of list, select the number of days.

Step 5 Click **View**. The report is displayed:

Column	Description
IP Address	The IP address of the access point or bridge.
Timestamp	The time the access point was last seen by the system.
Number of Associations	The number of client associations.
RF Utilization	The amount of radio frequency utilization.
Ethernet Utilization	The amount of Ethernet utilization.

Step 6 To export the report, click **Export.** (See Exporting a Report, page 4-28.)

Step 7 To email the report, click **Email Report**. (See Emailing a Report, page 4-28.)

Exporting a Report

Step 1 Click **Export**. An Export window appears.

Step 2 From the Output Format list, select the format in which you want the file exported: CSV, PDF, or XML.

Step 3 Click **Submit**. A window opens in the requested format and displays the output.

Emailing a Report

Procedure

Step 1 Click **Email Report**. A the right pane refreshes with an Email properties dialog box.

Step 2 Enter the following:

Field	Description
To	Enter the email address of the person to whom you want to send the report. An entry in this field is required.
Cc	Enter email addresses of persons that you want to copy on the email.
Subject	Enter a subject for the email.
Attachment Type	From the list, select the format in which you would like the report sent: CSV, PDF, or XML.
Message	Enter any message you would like to send.
Report Data for Last 'N' Days	This entry is applicable for Trends reports only. From the list, select the number of days for which you want report data emailed.

Step 3 To cancel the email, click **Cancel**.

Step 4 To send the email immediately, click **Send Now**.

Step 5 To schedule the email for later:

a. Click **Schedule**. The schedule job dialog box appears.

b. Enter the following:

Field	Description
Job Name	Enter a name for the job. For more information, see Naming Guidelines, page A-1.
Start Date	From the list, select the date you would like to send the email.
Start Time	From the list, select the time you would like to send the email.
Repeat	
Enable	Check if you want to set up a scheduled job that periodically sends email.
Every	From the list, select the period of time you would like the email sent.

Step 6 Do one of the following:

- Click **Cancel** to cancel the schedule.
- Click **Finish** to complete scheduling. You receive a confirmation message that your email has been scheduled.

To view, delete, or edit the scheduled email jobs, see Scheduling Email Jobs, page 4-29

Scheduling Email Jobs

This window allows you to view information about email jobs you have scheduled. It also allows you to delete them and edit them.

The length of time job data is retained is 30 days by default. To change the default setting, see Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Reports > Scheduled Email Jobs**. The Email Jobs window appears.

Field	Description
Job Name	The name of the job. For more information, see Naming Guidelines, page A-1.
Recurring	Indicates whether it is a recurring job.
Next Schedule	Indicates when the job runs again.

Step 2 To sort table data, click on the column heading you want to use to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Step 3 To delete a job, select it, then click **Delete Email Job**.

Step 4 To view an email job, select it, then click **View Email Job**. (See Viewing Email Job Details, page 4-31.)

Step 5 To edit a job, select it, then click **Edit Email Job**. The email appears and allows you to change any of the entries. (See Emailing a Report, page 4-28 for more information.)

Viewing Email Job Details

The following tables are displayed in a window when you select a job in **Reports > Scheduled Email Jobs**, then click **View Email Job**.

Report Properties

Column	Description
User Name	The name of the user who scheduled the job.
Report Type	The report type.
Report Name	The report name.

Email Properties

Column	Description
To	The username of the person to whom the report is being emailed.
Cc	The username of the person to whom the report is being copied.
Subject	The email subject.
Format	The format in which the report is being emailed.
Body	The text entered into the body of the email.

Schedule Properties

Column	Description
Email Job Name	The name of the email job.
Start Date	The date the report is emailed.
Frequency	The frequency with which the report is to be emailed.

CHAPTER 5

Performing Administrative Tasks

The Administration tab allows you to you perform administrative tasks.

Note Some of the subtabs may not be visible to some users; what you view under the Administration tab depends on your login.

The Administration subtabs have the following functions:

- **Discover**—Manage devices, configure discovery, specify device credentials, import devices, and set up LEAP servers (see Using Discovery and Managing Devices, page 5-2).
- **Group Management**—Place devices in groups for efficient management (see Managing Groups, page 5-28).
- **Appliance**—Manage the Wireless LAN Solution Engine server (see Managing the Appliance, page 5-34).
- **System Parameters**—Configure parameters for reporting performance and fault data (see Managing System Parameters, page 5-58).
- **User Admin**—Manage users and user roles (see Administering Users, page 5-60).
- **My Profile**—Change your password (see Modifying Your Profile, page 5-65).
- **Connectivity**—Test device connectivity and reachability and troubleshoot nonresponding devices (see Using Connectivity Tools, page 5-66).

Using Discovery and Managing Devices

The Discover window contains the following options:

- **Discover**—Set up discovery, perform an immediate discovery, and view discovery history (see Managing Device Discovery, page 5-2).
- **Managed Devices**—View newly discovered devices, change device status, and view device management history (see Managing Devices, page 5-13).
- **Inventory**—Run a one-time, immediate inventory to collect information from managed devices before the next *scheduled* inventory (see Running Inventory Now, page 5-17)
- **Device Credentials**—Specify community strings and specify the HTTP username and password for access points (see Setting Device Credentials, page 5-17).
- **Import Devices**—Import devices from a file or from a CiscoWorks2000 server (see Importing Devices, page 5-21).
- **Export Devices**—Export devices to a CiscoWorks2000 server (see Exporting Devices, page 5-24).
- **LEAP Server**—Add, modify, or delete LEAP servers (see Managing LEAP Servers, page 5-26).

Managing Device Discovery

The discovery options are:

- **Modify Discovery Settings**—Set up scheduled discoveries (see Add Seed Devices and Schedule Discovery, page 5-10).
- **Run Discovery Now**—Run a one-time, immediate discovery (see Run Discovery Now, page 5-11)
- **Discovery History**—View discovery details (seeView Discovery History and Status, page 5-12).

Related Topics

- Overview: Discovery, page 5-3
- Set Up Devices, page 5-4

Overview: Discovery

You can set up regularly scheduled discoveries and run one-time discoveries.

Before the WLSE can discover devices:

- You must configure discovery on the WLSE. See Add Seed Devices and Schedule Discovery, page 5-10.

  As an alternative to using Cisco Discovery Protocol (CDP) to run discovery, you can import devices from a file or from CiscoWorks2000. See Importing Devices, page 5-21.
- Devices must be properly configured for access by the WLSE. See Set Up Devices, page 5-4.
- Community strings must be entered on the WLSE. See Specify Community Strings, page 5-18).

Note Routers and switches are only discovered if they have properly configured access points attached to them.

Discovery proceeds according to the seed devices and CDP distance that you specify. The CDP distance determines the depth of the discovery. With a CDP distance of 1, only the immediate neighbors of the seed device are discovered. With a CDP distance of 2, devices A and B that are directly connected to the seed device are discovered, and the immediate neighbors of A and B are also discovered. You should set the CDP distance so that your entire wireless network is discovered.

After devices are discovered, you must move them to the managed state. Unmanaged devices do not appear in WLSE displays.

Related Topic

Importing Devices, page 5-21

Managing Devices, page 5-13

Set Up Devices

You must set up devices so the WLSE can discover and manage them. This section describes both required and optional setup tasks for:

- Access Points and Bridges, page 5-4
- Routers and Switches, page 5-7
- LEAP Servers, page 5-9

Access Points and Bridges

Before you begin, Web browsing must be enabled on each access point. If Web browsing is not enabled, attach a console to the access point and enable web browsing.

On each access point and bridge, open a web browser session on the device and perform the tasks in the following table.

Tasks	Procedure	Notes
1. Enable Cisco Discovery Protocol (CDP).	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services: Cisco Services, click **Cisco Discovery Protocol**. The CDP Setup page appears. 3. Select Enabled. Click **Apply** or **OK**.	CDP is required for the WLSE to discover devices on the network.
2. Enable SNMP. (Optional) Set the location. (Optional) Set the system name and system contact.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **SNMP**. The SNMP Setup page appears. 3. Select Enabled. 4. Enter a System Name, System Location, and System Contact. 5. Click **Apply** or **OK**.	SNMP is required for the WLSE to discover and manage the device. Setting the location enables proper grouping of devices into the system-defined Location group. For more information, see Managing Groups, page 5-28. Setting the system name and system location displays this information when you display device details.

Tasks	Procedure	Notes
3. Set the community string by creating a user with all privileges. (If you already entered an SNMP Admin Community name, the user created has Write, SNMP, Firmware, and Admin privileges, and the User Manager is enabled, you do not need to create another user.)	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **Security**. The Security Setup page appears. 3. Click **User Information**; then click **Add New User**. The User Management window appears. 4. To create an user with SNMP read/write privileges, enter a username and password and select the Write, SNMP, Firmware, and Admin capabilities. 5. Click **Apply** or **OK**.	The username of the user with Write and SNMP privileges is used as the SNMP read/write community string. The Firmware privilege is required for configuring devices from the WLSE.

Tasks	Procedure	Notes
4. Add an HTTP user with the ability to modify firmware, and enable the User Manager. You can use the same user that you created in Task 3, if the user has firmware privileges.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Click **Security**. The Security Setup page appears. 3. Click **User Information**; then click **Add New User**. The User Management window appears. 4. Enter a username and password and select Firmware; then click **Apply**. 5. Navigate back to the Security Setup page and click **User Manager**. The User Manager Setup window appears. 6. Select Enabled; then click **Apply** or **OK**.	This allows configuration uploads from the WLSE to the access point. All access points must be configured with the same HTTP user and password. You also enter this user and password on the WLSE (see Specify the HTTP Username and Password, page 5-20).
5. Set up TFTP as the transfer protocol between the WLSE and access points.	1. In the Summary Status page, click **Setup**. The Cisco Services Setup page appears. 2. Under Services, click **FTP**. The FTP Setup page appears. 3. Use the pulldown menu to select TFTP as the file transfer protocol. 4. In the Default File Server text box, enter the IP address of the WLSE. 5. Click **Apply** or **OK**.	TFTP is used for transferring configuration changes to access points.

Routers and Switches

Note Only routers and switches that have properly configured access points or bridges attached to them will be discovered.

On each router and switch, configure the following:

Task	Procedure	Notes
1. Enable CDP and verify that access points and bridges are visible from the router or switch.	1. Enter enable mode. 2. Verify that CDP is running on the switch or router: On IOS-based devices, use the **show cdp run** command. On Hybrid OS-based Catalyst switches, use the **show cdp** command 3. If CDP is not running, use the **set cdp enable** command to enable CDP. 4. To verify that access points or bridges are visible in the device's CDP table, use the **show cdp neighbors** command.	CDP is required for the WLSE to discover the device.

Task	Procedure	Notes
2. Enable SNMP and set up community strings.	On IOS-based devices, enter configuration mode and use the **snmp community** *community_string* **ro** command. On Hybrid OS-based Catalyst devices, enter enable mode and use the **set snmp community read-only** *community_string* command.	SNMP is required for the WLSE to discover and manage the device.
3. (Optional) Set the system name, contact, and location variables.	On IOS-based devices, enter configuration mode and use the following commands. • To set the system name, use the **hostname** *name* command. • To set the system contact, use the **snmp contact** *contact* command. • To set the location, use the **snmp location** *location* command. On Hybrid OS-based Catalyst switches, enter enable mode and use the following commands: • To set the system name, use the **set system name** *name* command. • To set the system contact, use the **set system contact** *contact* command. • To set the location, use the **set system location** *location* command.	These variables make the device more manageable. The location variable enables proper grouping of devices into the system-defined Location group. For more information about groups, see Managing Groups, page 5-28. The system name, system contact, and location will appear in the device detail displays.

LEAP Servers

The WLSE can monitor a LEAP server (CiscoSecure ACS Server) that provides LEAP services to a wireless LAN using synthetic transactions.

Note Each LEAP server must be specified on the WLSE. For more information, see Managing LEAP Servers, page 5-26.

Procedure

To set up a LEAP server and add the WLSE as a Network Access Server (NAS) on the LEAP server:

Step 1 Log into the CiscoSecure ACS Server.

Step 2 Click **User Setup** on the left side of the initial page. The User Setup page appears.

Step 3 In the User text box, enter the name of the user that the WLSE will use for synthetic transactions.

Step 4 Click **Add/Edit**; then enter the appropriate information for the user, including the password. Click **Submit**.

Step 5 Click **Network Configuration** on the left side of the page. The Network Configuration screen appears.

Step 6 Click **Add Entry**. The Add Access Server screen appears.

Step 7 Enter the WLSE information in the following text boxes:

- Network Access Server Hostname
- Network Access Server IP
- Key (the shared key)

Step 8 Select RADIUS (Cisco Aironet) from the Authenticate Using list.

Step 9 Click **Submit** or **Submit+Restart**. A restart is required for the changes to take effect.

Add Seed Devices and Schedule Discovery

Neighbors of seed devices are discovered by examining the contents of CDP tables. Before discovery can proceed, you must specify at least one seed device. Any supported device can function as a seed.

You may want to specify multiple seed devices to:

- Shorten the discovery time.
- Discover "disconnected" networks; that is, discover devices across links on which CDP is disabled or discover devices outside the firewall.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Discover > Modify Discovery Settings**.

Step 2 To delete a seed device, select the IP address from the Seed Values list and click **Delete**.

Step 3 To add a seed device, enter its IP address in the Seed Values text box and click >>.

Note Before you can modify the discovery schedule, you must have at least one seed device in the Seed Values list.

Step 4 Repeat step 3 to add more seed devices.

Step 5 Select the CDP distance from the list. Set CDP distance appropriately to discover the entire wireless network; a CDP distance of 1 only discovers the immediate neighbors of the seed devices.

Note Routers and switches that do not have access points attached to them are used when computing CDP distance. However, such devices will not appear in the discovered devices list.

Step 6 To schedule discovery, click **Next: Modify Schedule**. The Modify Discovery Schedule dialog box appears.

- Select the State Date and Start Time from the pulldown lists.
- To repeat discovery at specified intervals, click **Enable**. Then enter a number and select the interval from the Every list.

Step 7 Click **Next**. The CDP Discovery - Summary dialog box appears.

Step 8 Click **Finish** to submit your settings or **Back** to make changes in your settings.

Run Discovery Now

This option allows you to run an immediate one-time discovery.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Discover > Run Discovery Now**. The Discovery - Seeds dialog box appears.

Step 2 If necessary, add seed devices:

Note If you add seed devices in the Discovery - Seeds dialog box, they will not be saved. Any seed devices added here are used for this one-time discovery only.

a. Enter the seed device's IP address in the Add Seed Value text box and click >>.

b. Set the CDP distance by selecting a number from the list.

Step 3 Click **Run Now**. The Discovery - Summary dialog box appears.

- Click **Back** if you want to make changes.
- Click **Finish** to run the discovery. The discovery will begin within 2 minutes.

View Discovery History and Status

The Discovery History table shows completed and scheduled discovery jobs.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Discover > Discovery History**. The Discovery History table appears:

Field	Description
Discovery Name	The job name. The scheduled discovery is called CDPDiscovery. One-time discoveries and discoveries initiated by device imports are called CDPDiscovery_*type_number*; for example, CDPDiscovery_Import_Devices_4.
Recurring	Whether the job is recurring.
Schedule Time	The next time the job will run.

Note If the Discovery History table grows too large, you can reset the Job History Truncation Interval parameter in **Administration > System Parameters** so that the table is truncated more often. For more information on this parameter, see Managing System Parameters, page 5-58.

Step 2 From the Discovery State list, select the discoveries you want to view: scheduled discoveries, discoveries that are currently running, or all discoveries. The Discovery History table is displayed.

Step 3 To view more information about a discovery in the Discovery History table, select the radio button and click **Discovery Run Detail**. This Discovery Run Details window appears, showing the Discovery Start and End times.

Step 4 To view the detailed log for a particular discovery run, select the run and click **Discovery Run Log**. The following information is displayed in the Discovery Run Log:

- The seed devices used.
- The CDP distance configured for the seed devices.
- When the discovery started and ended (displayed as UTC).
- The number of devices that were discovered or rediscovered.
- A list of the devices that were discovered. Devices listed as *being updated* were already discovered in a previous discovery run.
- A list of devices that were previously discovered but are now unreachable.
- Devices that are unreachable because CDP is not enabled on the device or SNMP is not configured on the device.

Step 5 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Managing Devices

Before you can view devices or perform any operations on them, you must move the devices to the managed state. The device management options are:

- **Manage/Unmanage**—View newly discovered devices, change device management status, or delete devices (see Manage Devices, page 5-13).
- **Device History**—View the management history of each discovered device (see View Device Management History, page 5-16).

Manage Devices

You can use this option to change a device's management status or delete a device.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration** > **Discover** > **Managed Devices** > **Manage/Unmanage**. The device selector is displayed, showing:

- Newly discovered devices (New folder). All new devices are also listed in the Unmanaged folder.
- Managed devices (Managed folder)
- Unmanaged devices (Unmanaged folder).

Step 2 To view the contents of a folder, expand the folder.

Step 3 To modify the status of the devices in a folder, click the folder name. The Group Status pane appears. Select one or more devices from the list and click **Manage** or **Unmanage** in the Group Change Status window. Devices are moved into the Managed or Unmanaged folders.

You must move newly discovered devices to the managed state. Only managed devices appear in WLSE displays.

Note You can only manage a total of 525 access points and wireless bridges. After you have placed 500 of these devices into the Managed folder, warning messages are displayed when you place more devices in the folder. After the 525 limit is reached, no more devices can be placed in the Managed folder. Discovery of access points and wireless bridges is not limited to 525 devices.

Step 4 After you move devices to the managed state, it is recommended that you run inventory. This ensures that devices appear in displays such as reports and system-defined groups without waiting for the next inventory cycle. To run inventory:

a. Select **Administration** > **Discover** > **Discover** > **Inventory**.

b. Click **Run Inventory**.

For more information, see Running Inventory Now, page 5-17.

Step 5 To view details about a device, select the device from the device selector. The Device Details pane appears. You can change the device's status by using the Manage and Unmanage buttons.

Note Some details may not be displayed if the corresponding parameters are not set on the device; for example, Location and Contact.

The details in the Device Details pane are:

Field	Description
Device Name	Hostname or IP address.
Description	Detailed device description.
Version	Software version installed on the device.
Device Family	Device type.
SysName	The system name.
SysObjectId	Unique identifier that identifies the device type.
Location	Where the device is located.
IP Address	Device IP address.
Subnet	Subnet in which the device is located.
Network Segment	The network segment in which the device is located.
Contact	The person to contact for this device.

Step 6 To delete a device, select the device from the device selector or dialog box and click **Delete**.

The device will be removed from the device selector and from all tables (including trend tables).

Related Topics

Managing Device Discovery, page 5-2

View Device Management History

The Historical Operations table shows information on all changes in device state (from unmanaged to managed or vice versa).

Note Your login determines whether you can use this option.

Procedure

Step 1 To view the Historical Operations table, select **Administration > Discover > Managed Devices > Device History**. The following information is displayed:

Field	Description
Timestamp	Date and time when the state change occurred.
Device Name	The device's hostname.
IP Address	The device's IP address.
State	The device's state: • New—Device was discovered but has not been moved to the managed or unmanaged state. • Managed—Device has been moved to the managed state. • Unmanaged—Device is unmanaged.

Step 2 To sort table data, click on the column heading by which you want to sort the data:

- A triangle indicates ascending order.
- An upside-down triangle indicates descending order.
- No triangle indicates that the data is not sorted.

Running Inventory Now

By default, the WLSE collects device configuration information every hour. You can use this option to run a one-time, immediate inventory. Running an immediate inventory after you move devices to the managed state is recommended so you can see the devices in displays such as reports and system-defined groups, without waiting for the next scheduled inventory cycle.

To change the scheduled inventory interval, you can reset the Inventory Polling Interval parameter. See Managing System Parameters, page 5-58.

Note Your login determines whether you can use this option

Procedure

Step 1 Select **Administration > Discover > Discover > Inventory**.

Step 2 Click **Run Inventory**. The inventory job will start within 2 minutes. A confirmation message appears, managed devices are polled, and configuration information is collected. WLSE displays will be updated accordingly.

If a scheduled inventory or previous immediate inventory is already running, a message appears. You should wait for the running inventory to complete before starting another immediate inventory.

Setting Device Credentials

This option allows you specify device community strings and HTTP credentials.

- **SNMP Communities**—Specify community strings for managed devices. See Specify Community Strings, page 5-18.
- **HTTP User/Password**—Specify the HTTP username and password for configuring access points. See Specify the HTTP Username and Password, page 5-20.

Specify Community Strings

The Wireless LAN Solution Engine uses a device's read-only community string for discovery and the read/write community string to configure the device. If community strings are not entered correctly, the Wireless LAN Solution Engine cannot communicate with the device. Both read-only and read/write community strings are required.

The default community string is *public* for both the read-only string and the read-write string. If the community strings on your devices differ from the defaults, you must specify the community strings before the discovery process can begin and before you can configure the devices.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Device Credentials > SNMP Communities**. The Bulk SNMP Settings dialog box appears.

This dialog box contains a default entry that covers all devices, provided device community strings are set to the default (*public*).

Step 2 Add new entries or modify existing entries in the text box using the following syntax:

target:*read_community*::*timeout*:*retries*:::*write_community*

Note You must enter the correct number of colons between variables. Otherwise, the community strings cannot be read.

Information about the variables follows. For more details, see Community String Guidelines, page 5-20.

Variable	Description	Notes
target	A device or range of devices that use these community strings.	If you do not specify a target, the default community strings apply to all devices in the network.
read_community	A password allowing read-only access to the target devices.	You must specify a read community string. Otherwise, the default value of public is used.
timeout	The length of time (seconds) the server waits for a response from the device before performing the first retry.	The default is 10 seconds. If you increase the timeout period, discovery could take significantly longer to complete. The minimum value is one and the maximum value is 60.
retries	The number of times the server attempts to communicate with the device before declaring that the device has timed out.	The default is one retry. If you increase the number of retries, discovery takes significantly longer to complete. The default retry policy doubles the previous timeout value for retry.
write_community	The password that allows write access to the target devices.	You must specify the write community string. Otherwise, the default value of public is used.

Step 3 Select **Reverse DNS Lookup** if DNS is configured on the device.

- If DNS Lookup fails, the device IP address will be used; however, discovery will take longer.
- If DNS Lookup succeeds, the WLSE displays will show the device's hostname instead of the IP address in device name fields.

Step 4 Click **Save** to apply your changes.

Related Topic

Community String Guidelines, page 5-20

Community String Guidelines

Use these guidelines when adding or modifying community strings:

- You can assign community strings to any of the following:
  - Complete IP address; for example, 172.20.4.9
  - Any wild cards (based on IP addresses); for example:

    ..*.*

    172.*.*.*
  - Address ranges, which can include wild cards; for example:

    27.20.[4-55].*

    172.[21-30].[44-88].*

    172.*.*.[121-255]
- You can add a combination of general and specific entries, but the Wireless LAN Solution Engine reads the community strings from most specific to least specific.
- If you enter duplicate community strings for a device, the most specific community string is used.
- A # sign as the first character on a line indicates a comment.
- All printable characters, except for colons (:), are allowed in community strings.
- Spaces are not allowed in community strings.

Specify the HTTP Username and Password

The HTTP username and password are required for downloading configuration files to access points. The password must be set on each access point. For more information, see Set Up Devices, page 5-4.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Device Credentials > HTTP User/Password**.

Step 2 Enter a username or modify the username in the User field.

Step 3 Enter or modify the password in the Password field.

Step 4 Enter or modify the password in the Confirm Password field.

Step 5 Click **Save**.

Related Topic

Chapter 3, "Configuring Devices"

Importing Devices

Instead of running discovery on the WLSE, you can import devices:

- From a file (see Import Devices from a File, page 5-22).
- From CiscoWorks2000 Resource Manager Essentials (see Import Devices from CiscoWorks2000, page 5-23).

A one-time discovery job starts within 2 minutes after you import devices. All WLSE-supported devices in the file are used as seed devices with a CDP distance of 1. These devices are not added to the list of available seed devices in the Discovery - Configuring Seeds dialog box, but they do appear in the Discovery Run Log. See Add Seed Devices and Schedule Discovery, page 5-10 and View Discovery History and Status, page 5-12.

Devices not supported by the WLSE are ignored.

You can choose to discover some devices and import others.

The following information is imported:

- IP addresses are accepted, and hostnames are resolved to obtain the IP address. Hostnames that cannot be resolved are ignored.
- Read-only and read/write community strings are appended to the end of the Bulk SNMP Settings table (**Administration > Discover > Device Credentials**). See Setting Device Credentials, page 5-17.

Note Imported credentials are not matched with existing entries that contain wildcards or ranges.

Import Devices from a File

You can import devices from a file that contains device information in the CSV format. You can create a CSV file by exporting devices from CiscoWorks2000 or by creating the file with a text editor. You can view a sample CSV file in the dialog box for importing files.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Import Devices > From File**. The Import Devices from File dialog box appears.

To see a sample file, click **See Sample CSV File**.

Step 2 You can enter a pathname for the file in the Choose File dialog box or click Browse to find the file in the client directory structure.

Step 3 Click **Import**. Devices are imported and a one-time discovery begins within 2 minutes.

Step 4 To verify the discovery, see View Discovery History and Status, page 5-12.

Related Topics

- Import Devices from CiscoWorks2000, page 5-23
- Add Seed Devices and Schedule Discovery, page 5-10
- Setting Device Credentials, page 5-17
- View Discovery History and Status, page 5-12

Import Devices from CiscoWorks2000

You can import devices directly from CiscoWorks2000 by connecting to a CiscoWorks2000 server.

The time required to import devices depends on the response from the CiscoWorks2000 server and the number of devices imported. The following procedure explains how to check the status of the operation.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Import Devices > From CiscoWorks2000**.

Step 2 Enter the following information. All fields are required; if any are left blank, the display will clear.

- The CiscoWorks2000 server IP address.
- The port number at which the CiscoWorks2000 server listens for HTTP requests. You may need to contact the administrator of the CiscoWorks2000 server to obtain this information.
- The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

Click **Import**. After devices are imported, a one-time discovery begins.

Step 3 To see the Import Status log, click **Status**. The CiscoWorks2000 Import Status window appears. To refresh the status display, click **Refresh**.

- If the Last Status button is displayed in place of the Status button, you can review the results of a previous import.
- If the import fails because you entered the wrong data in the Import dialog box, one of the following error messages is included in the Import Status log:
  - The following message means that either the host or the port specified in the WLSE import dialog was wrong:

    Error: Could not connect to CiscoWorks2000 server:*ip_address* on port:*port_number.*

  - The following message means that either the user or password specified in the WLSE import dialog was wrong:

    Error: Connected to CiscoWorks2000 server:*ip_address* on port:*port_number* successfully, but server returned error after connection.

- If the import succeeds, you can view detailed information in the Discovery Run Log. See View Discovery History and Status, page 5-12.

Related Topics

- Import Devices from a File, page 5-22
- Add Seed Devices and Schedule Discovery, page 5-10

Exporting Devices

You can export all WLSE-discovered devices to a CiscoWorks2000 server running Resource Manager Essentials. The information exported consists of the device IP addresses and their credentials.

The time required to export devices depends on the number of devices exported and the response from the CiscoWorks2000 server. The following procedure explains how to check the status of the operation.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > Export Devices > To CiscoWorks2000**.

Step 2 Enter the following information:

- The CiscoWorks2000 server IP address.
- The CiscoWorks2000 server port number. You may need to contact the administrator of the CiscoWorks2000 server.
- The username and password of any user who has the authority to export and import device credentials on the CiscoWorks2000 server.

Step 3 Click **Export**.

The Export to CiscoWorks2000 Started window appears.

Step 4 To see the export status log, click **Status**. The CiscoWorks2000 Export Status window appears. To refresh the status display, click **Refresh**.

If the Last Status button is displayed in place of the Status button, you can review the results of a previous export.

The following information is included in the export status log:

Type of Information	Description
Device information	Name of the device, device status, and device status details. The string !{[NO VALUE]}! does not indicate an error; it means information was not available to the CiscoWorks2000 server while it was sending a response to the WLSE.
Error messages	The following message means that either the host or the port specified in the WLSE export dialog was wrong: Error: Could not connect to CiscoWorks2000 server:*ip_address* on port:*port_number*.
	The following message means that either the user or password specified in the WLSE export dialog was wrong: Error: Connected to CiscoWorks2000 server:*ip_address* on port:*port_number* successfully, but server returned error after connection.

After you export devices, you can view the exported devices in CiscoWorks2000 Resource Manager Essentials (see the Resource Manager Essentials online help for details).

Managing LEAP Servers

This window allows you to manage LEAP servers (CiscoSecure ACS Servers). LEAP servers monitor the authentication servers, detecting performance problems and ensuring availability. LEAP servers must be configured for synthetic transactions.

After you save LEAP server credentials, the WLSE automatically performs periodic LEAP logins to monitor the response time and availability of LEAP servers. To change the default polling interval and fault thresholds, select **Faults > Specify Fault Thresholds > LEAP > Response Time**.

A LEAP server must be set up for LEAP logins. For information on setting up LEAP servers, see Set Up Devices, page 5-4.

You can use the LEAP server options to:

- Add a LEAP Server, page 5-26
- Modify a LEAP Server, page 5-27
- Remove a LEAP Server, page 5-28

Related Topics

- Setting LEAP Server Response Time, page 2-12
- Displaying Faults, page 2-1
- Specifying Fault Thresholds, page 2-7
- Specifying Policies, page 2-13
- Forwarding Faults, page 2-15

Add a LEAP Server

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > LEAP SERVER > Add Server**. The LEAP Server: Add Server dialog box appears.

Step 2 Complete the following:

Text Box	Description
Server Name	Enter the name of the server.
Server Port	Enter the number of the port the server uses for authentication.
Username	Enter the LEAP username.
Password	Enter the LEAP password.
Secret	Enter the shared secret key.

Step 3 Click **Submit** to apply your settings, or **Reset** to apply the default values.

Modify a LEAP Server

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > LEAP Server > Modify Server**. The LEAP Server: Modify Server dialog box appears.

Step 2 Modify attributes as desired:

Text Box	Description
Server Name	From the list, select the server name you want to modify.
Server Port	Modify the port number used for authentication.
Username	Change the LEAP server name.
Password	Change the LEAP password
Secret	Change the shared secret.

Step 3 Click **Submit** to apply your settings, or **Reset** to apply the default values.

Remove a LEAP Server

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Discover > LEAP Server > Remove Server**. The LEAP Server: Remove Server dialog box appears.

Step 2 From the list, select the server you want to remove, then click **Submit**.

Managing Groups

This window contains a group selector and a dialog box for creating, editing, and deleting groups.

Related Topics

- Overview: Groups, page 5-28
- Creating, Editing, and Deleting Groups, page 5-29

Overview: Groups

The Group Management window allows you to view the existing device groups and categorize devices into named groups so that you can perform management tasks on a group of devices as a single operation.

A group is a named entity consisting of a set of devices, a set of groups, or a combination of devices and groups. A group can consist of both user-defined groups and system-defined groups.

There are five folders containing system-defined groups. You cannot edit or delete a system-defined group. The system defined groups are automatically populated using information read from the devices during discovery and inventory collection. Any changes on devices are reflected in the system-defined groups only after the next discovery or inventory collection has completed. The system-defined groups and folders are:

- Device Type folder—Contains groups for 1200 APs, 340 APs, 350 APs, 350 Bridges, Routers, and Switches.
- Location folder—Contains groups based on the locations of the devices. To enable creation of system-defined location groups, you must configure a parameter on the device that identifies the device location. See Set Up Devices, page 5-4 for information on setting location. The null location group contains all devices that are not configured with their location information.
- SSID folder—Contains a group for each radio service set ID (SSID) configured on access points. For information on configuring the SSID, see Set Up Devices, page 5-4
- Subnet folder—Contains a group for each subnet configured in the network.
- Software Version folder—Contains a group for each software version detected on the devices.

Related Topics

- Managing Device Discovery, page 5-2
- Running Inventory Now, page 5-17

Creating, Editing, and Deleting Groups

You can create groups and edit or delete groups that were created by users. The system-defined groups cannot be edited or deleted.

Use the options in the Group Management window to:

- Add a Group, page 5-30
- Edit a Group, page 5-32
- Delete a Group, page 5-33

To view the devices in a group, select **Administration > Group Management**. Click a group folder in the group selector in the left pane. The group name, description, creator, and devices are listed in the Group window.

Add a Group

You can add groups by:

- Creating a New Group, page 5-30
- Copying an Existing Group, page 5-31

Note Your login determines whether you can use this option.

Creating a New Group

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and group window are displayed.

The group selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder shows how many devices are in the group or how many groups are in the folder. Every managed device appears in one or more of the system-defined groups, and may also appear in user-defined groups.

Step 2 To create a new group, click **Create New**. The Create Group dialog appears.

Step 3 Enter a name in the Name text box. Enter a description in the Description text box (optional).

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 4 From the group selector in the left pane, select a group that contains devices you want to add to your new group. Devices in that group are added to the All Available Devices list in the Create Group dialog.

Step 5 To add devices to the new group, select the group or individual devices from the All Available Devices list and click **Add** >>. Devices are moved to the Devices in Group list.

Step 6 To add more devices to the new group, repeat Steps 4 and 5.

Step 7 To remove devices from the group, select them from the Devices in Group list and click **Remove**.

Step 8 To save the group, click **Save**. The new group is displayed and added to the end of the group selector list. To cancel the group creation and discard your changes, click **Cancel**.

Copying an Existing Group

Use this procedure to create a new group by copying an existing group.

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and group dialog box are displayed.

The group selector lists all the current groups, both system-defined groups and user-defined groups. The number after a group name or folder show how many devices are in the group or how many groups are in the folder. Every discovered and managed device appears in one or more of the system-defined groups, and may also appear in user-defined groups.

Step 2 To copy an existing group, select the group and click **Copy**. The Copy Group dialog appears. The devices in the group are placed in the Devices in Group list.

Step 3 Edit the name, if desired. Add a description in the Description text box (optional).

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 4 To add more devices to the group, select another existing group. Devices in that group are added to the All Available Devices list in the Create Group dialog.

Step 5 Select the group or individual devices from the All Available Devices list and click **Add** >>.

Step 6 To add more devices, repeat Steps 4 and 5.

Step 7 To remove devices from the group, select them from the Devices in Group list and click **Remove**.

Step 8 To save the group, click **Save**. The new group is displayed and added to the end of the group selector list. To cancel the group creation and discard your changes, click **Cancel**.

Related Topics

- Edit a Group, page 5-32
- Delete a Group, page 5-33
- Overview: Groups, page 5-28

Edit a Group

You can edit user-defined groups, but system-defined groups cannot be edited.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Group Management**. The group selector pane and Group dialog box appear.

Step 2 Select a group to edit from the group selector in the left pane and click **Edit**. The Edit Group dialog appears.

Step 3 Change the Name or Description by editing the text in the text boxes.

For information about the characters allowed in group names and descriptions, see Naming Guidelines, page A-1.

Step 4 To add devices to the group, select a group from the group selector. The devices in the group appear in the All Available Devices list. Select the group or individual devices from the list and click **Add**. Devices are placed in the Devices in Group list.

Step 5 To add more devices, repeat Step 4.

Step 6 To delete devices from the group, select one or more devices from the Devices in the Group list and click **Remove**.

Step 7 To save your changes, click **Save**. The edited group is displayed. To discard your changes, click **Cancel**.

Related Topics

- Add a Group, page 5-30
- Delete a Group, page 5-33
- Overview: Groups, page 5-28

Delete a Group

You can delete user-defined groups, but you cannot delete system-defined groups.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Group Management**. The group selector appears in the left pane and the Group window appears.

Step 2 Select the group from the group selector list. The group is displayed.

Step 3 Click **Delete**.

Related Topic

- Overview: Groups, page 5-28
- Edit a Group, page 5-32
- Add a Group, page 5-30

Managing the Appliance

The Appliance window contains the following options:

- **Status**—Gather and view WLSE statistics and restart the machine (see Viewing WLSE Status, page 5-34).
- **Software—**Update, reinstall, view status, and define the repository for the WLSE software (see Managing the Software, page 5-37).
- **Security**—Manage the WLSE security features, such as telnet, SSL, authentication modules (see Managing Security, page 5-45).
- **Backup and Restore**—Configure backup location, backup data, and restore data (see Backing Up and Restoring Data, page 5-50).
- **Diagnostics**—Troubleshoot, run self-tests, view process status (see Using Diagnostics, page 5-52).
- **Splash Screen**—Customize the splash screen message (see Setting Up the Splash Screen Message, page 5-57).

Note Your login determines whether you can use these options.

Viewing WLSE Status

The Status options include:

- Log file statistics (see Viewing Log File Reports, page 5-35).
- Restart (see Restarting the Wireless LAN Solution Engine, page 5-36).

Viewing Log File Reports

This option allows you to gather and view file system statistics.

Procedure

Step 1 Select **Administration > Appliance > Status > View Log File.** The Log File Utilities dialog box appears with the following information:

Field	Description
Log file	Name of the log file displayed.
Directory	Location of log file.
File Size	Size of file.
Size Limit	Recommended maximum file size.
File Size Utilization %	Percentage of the maximum size (500MB) being used.

Step 2 To see log file details, click the name of the log file. A window appears with log file information.

Step 3 To search for specific data within the log files, click the check boxes of the log files you want to search, and enter a keyword into the Keyword text box. Click **Case Sensitive** if you want your search to be case sensitive, then click **Search**. A window displays the results of the search.

Log Files Displayed

Log File	Content
access_log	Web server user access log.
daemons.log	Log file for logging messages that dmgtd does not log.
dmgtd.log	Process Management daemon log file.
error_log	Web server error log.

Log File	Content
faults.log	Log for device fault information.
install.log	Software package installation log.
jobvm.log	Log for all scheduled tasks.
mfgtest.log	Log for the manufacturing test.
mod_jk.log	Message log for hook between Tomcat and Apache.
snmpd.log	SNMP agent log file.
ssl_request_log	Log for secure socket layer web server events for https.
tomcat.log	Java servlet messages.

Restarting the Wireless LAN Solution Engine

This option allows you to restart the WLSE.

After the Wireless LAN Solution Engine restarts, discovery (see Managing Device Discovery, page 5-2) will begin immediately, the performance thresholds will resume collecting, the views will update, and all other functions will resume.

Procedure

Step 1 Select **Administration** > **Appliance** > **Status** > **Restart**. The Restart System screen appears.

Step 2 Click **OK** to restart the Wireless LAN Solution Engine.

Note If you need to perform a manual soft restart (for example, when modifying a network interface) you can use the CLI commands. (Refer to *User Guide for the CiscoWorks1105 Wireless LAN Solution Engine*—From the Online Help, click **View PDF**.)

Managing the Software

The Software options include:

- **Status**—Currently installed software information, such as software description, installation date, and installation status (see Viewing Software Status, page 5-37).
- **Define Repository**—Specify the repository location. The repository provides software update services to the WLSE (see Defining the Repository, page 5-38).
- **Software Updates**—Select and install a software update from the repository. You must specify the repository before updating software so the Wireless LAN Solution Engine can locate the software updates (see Installing Software Updates, page 5-41).
- **Browse Repository**—Browse the available complete images and software upgrades on the repository (see Browsing the Repository, page 5-43).
- **Software Update History**— Information about current and previous versions of installed software, including version number, install date, and installation status (see Viewing Software Update History, page 5-44).

Viewing Software Status

Procedure

Step 1 Select **Administration** > **Appliance** > **Software** > **Status**. The Software Status window appears with the Installed Software table, which contains the following information about all the software currently installed on the Wireless LAN Solution Engine:

Field	Description
Software Name	Brief description of the software.
Installation Date	Date and time (UTC) the software was installed.
Status	Status of the installation.
Details	Detailed install log for this software.

The Last Installation Information table displays the following about the most recent software installation:

Field	Description
Name	Brief description of the software.
Installation Status	Status of the installation.
Log File	Detailed install log for this software.

Step 2 To view details about an installation, click **View Log** in the Details field.

The install log for the selected installation opens. The information about the latest software installed is displayed.

Related Topics

- Viewing Software Update History, page 5-44
- Installing Software Updates, page 5-41
- Managing the Software, page 5-37

Defining the Repository

The repository warehouses the available software updates for the WLSE. The repository can be either local (on the Wireless LAN Solution Engine), or remote (on a Windows NT or Windows 2000 server). The default is a local repository.

By defining the repository, you are telling the WLSE where to look for available software updates. You can download software from the repository and install it on the Wireless LAN Solution Engine, and you can browse the available software versions on the repository.

However, before you can define the repository using the GUI, you must first create the repository:

- To create a local repository, see Creating a Local Repository, page 5-39.
- To create a remote repository, see Creating a Remote Repository, page 5-40.

Procedure

Step 1 Select **Administration > Appliance > Software > Define Repository**. The Define Repository dialog box appears.

Step 2 To define or redefine the repository, complete the following:

Text Box	Description
Host Name	The hostname or IP address of the repository. For the local repository, enter `localhost`.
Port Number	The port number used by the software on the repository. The default port number for the local repository is 9851.
Description	A description of the repository. This text box is optional; you can enter any description.

Step 3 Click **Connect to Repository** to verify that the hostname and port number you entered are correct. If the data is incorrect, an error message appears.

Related Topics

- Installing Software Updates, page 5-41
- Browsing the Repository, page 5-43
- Managing the Software, page 5-37

Creating a Local Repository

The repository warehouses the available software updates for the Wireless LAN Solution Engine. A single Wireless LAN Solution Engine can serve as the repository for itself and multiple other Wireless LAN Solution Engines.

To create a local repository, configure the repository using the CLI.

Note To use the local repository, you must be downloading software updates from an FTP site.

For more information, see *Installing and Configuring the Cisco 1105 Wireless LAN Solution Engine*, "Updating your Wireless LAN Solution Engine" section.

Procedure

Step 1 Open a CLI window to the Wireless LAN Solution Engine.

Step 2 Specify the source of the software updates. Use the following CLI command:

repository source ftp://*hostname/path*

The FTP site is the source for downloading software updates.

Step 3 Find the software you want on the FTP site.

Step 4 Download the software you want from the FTP site to the repository using the following command:

repository add *package*

Creating a Remote Repository

The repository warehouses the available software updates for the Wireless LAN Solution Engine. A remote repository can serve as the repository for one or more Wireless LAN Solution Engines. One Wireless LAN Solution Engine can function as the remote repository for other Wireless LAN Solution Engines, or the remote repository can be a Windows NT or Windows 2000 server. (A remote repository created on a Windows NT or Windows 2000 server will be temporary. It will not exist after the server reboots.)

Note If you are using a Wireless LAN Solution Engine as a remote repository, see Creating a Local Repository, page 5-39.

Procedure

Step 1 Download the ZIP file containing the update. The latest updates can be found at ftp.cisco.com.

Step 2 Extract the file to any empty directory. For example, extract the file to C:\hse\hse_repository.

Step 3 Open a command window and enter the following command:

```
subst <drive2:><drive1:>\<path>
```

Note Drive2 is a virtual drive. It will be removed after rebooting the Windows 2000 or Windows NT machine.

Step 4 Open <drive2:>.

Step 5 If Autoplay is enabled, the autorun.bat file will automatically run. If it does not, double-click it. A browser window opens, displaying the Appliance Update screen.

Step 6 Enter the hostname or IP address of the appliance.

The remote repository is now on the Windows NT or Windows 2000 server. To install software updates from this repository, see Installing Software Updates, page 5-41.

Related Topic

Creating a Local Repository, page 5-39

Installing Software Updates

Note When you update or reinstall software, the Wireless LAN Solution Engine stops and restarts. Therefore, you cannot access the Wireless LAN Solution Engine during a software update, and you must log in again after updating software.

Procedure

Step 1 Select **Administration > Appliance > Software > Install Software Updates**. The Install Software Updates window opens and displays information about the Wireless LAN Solution Engine, the currently defined repository, and the compatible software available for updating.

Step 2 Select a software version from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

These tables display the following information about the software you can install.

Field	Description
Name	Software identifier.
Version	Version number of the software.
Summary	Brief description of the software.
Release Date	Release date of the software.
Details	Detailed description of the software.

Step 3 To view details about any of the listed software, click **README** in the Details field.

Step 4 To begin the installation, make a selection from the Compatible Updates table, Compatible Reinstallations table, or Complete Images table.

Step 5 To install the selected software, click **Install**. The Install Software Updates window opens.

Step 6 Click **Confirm** to continue the installation. Click **Cancel** to cancel the installation.

When the installation is complete, the WLSE will be unavailable for a few minutes while it restarts. The Login screen will appear when the update is complete.

You can view details of the installation after the installation is complete (**Software > Status > View Log**).

Related Topics

- Defining the Repository, page 5-38
- Viewing Software Status, page 5-37
- Viewing Software Update History, page 5-44
- Browsing the Repository, page 5-43
- Managing the Software, page 5-37

Browsing the Repository

You can browse the available complete images and software upgrades on the repository using this option.

Note A repository must be defined in order to browse software. To define the repository, see Defining the Repository, page 5-38.

Procedure

Step 1 Select **Administration > Appliance > Software > Browse Repository**. The Browse Repository dialog box appears.

Step 2 To view detailed information about a complete image or update, click **README** in the Complete Images table or Updates table. These tables display the following about all the software available on the repository:

Field	Description
Name	Software identifier.
Version	Version number of the software.
Appliance Type	The appliance type that the software is designed for.
Release Date	Release date of the software.
Summary	Brief description of the software.
Details	Detailed description of the software. Click **README** to display details.

Related Topics

- Installing Software Updates, page 5-41
- Managing the Software, page 5-37

Viewing Software Update History

This window shows only the update history, not a history of installed images. If you install a complete new image, the previous update history will be erased.

Procedure

Step 1 Select **Administration > Appliance > Software > Software Update History**. The Software Update History window displays the following:

Field	Description
Name	Software identifier.
Version	Software version.
Summary	Summary of the installed software.
Install Date	The date and time (UTC) the software was installed.
Status	The status of the installed software.
Details	The detailed install log for this software.
Status	The status of the installation: Success—Software was installed with no errors. Warning—Software installed successfully with minor errors. Error—Software installation was unsuccessful.
Details	The detailed install log for this installation, including warning and error messages.

Step 2 Click **View Log** in the Details field to view the detailed install log for a software installation.

Related Topics

- Viewing Software Status, page 5-37
- Browsing the Repository, page 5-43
- Managing the Software, page 5-37

Overview: Security

The WLSE provides the following security features:

- Optional secure connection through a Web browser
- Connection through the CLI via Telnet
- Secure connection through the CLI via SSH
- Authentication through the local database or through alternative authentication services
- Flexible user access to managed devices and Wireless LAN Solution Engine services through configurable roles.

You can manage your system's security by:

- Selecting an Authentication Module, page 5-47
- Disabling or Enabling Telnet and Selecting SSH, page 5-49
- Viewing the Last 10 Logged-On Users, page 5-49
- Managing Roles, page 5-60

Managing Security

The Security options include:

- **Authentication Modules**—Choose the authentication module used (see Overview: Authentication Modules, page 5-46).
- **SSL (HTTPS)**—Obtain a permanent, signed Certificate Signed Request (see Managing SSL (HTTPS), page 5-48).
- **Telnet and SSH**—Configure Telnet and SSH settings (see Disabling or Enabling Telnet and Selecting SSH, page 5-49).

- **Last 10 Logins**—View information about the last 10 users who have logged on to the WLSE (see Viewing the Last 10 Logged-On Users, page 5-49).

Overview: Authentication Modules

The Wireless LAN Solution Engine provides a mechanism for authenticating users through the local authentication module and a local database of user IDs and passwords. Many network managers, however, already have an authentication service. To use your own authentication service instead of the local module, you can select one of the alternative modules:

- TACACS+
- Radius
- MS NT Domain

After you select and configure a module, all authentication transactions are performed by the authentication service associated with that module. Users log in with the user ID and password associated with the current authentication module.

The Wireless LAN Solution Engine determines user roles; therefore, all users must be in the local database of user IDs and passwords. A user's role determines the services and devices that the user can access. Users must have the same user ID locally as they have in the alternative authentication source, but the local password and authentication service password do not have to be same.

Users who are authenticated by an alternative service and who are not in the local database have no roles assigned to them. Users who have no roles see only the splash screen after logging in and cannot view screens or perform tasks.

If the alternative authentication service fails, the Wireless LAN Solution Engine defaults to the Local authentication module. Even if the local user database fails, you can always log in as the admin user.

Related Topics

- Selecting an Authentication Module, page 5-47
- Administering Users, page 5-60

Selecting an Authentication Module

The Local login module is selected by default, but you can select a different module.

Procedure

Step 1 Select **Administration > Appliance > Security > Authentication Modules**. The Authentication Modules dialog box appears.

Step 2 Select an authentication module from the Select Module drop down list, then click **Submit**. A Configuration dialog box appears for all selections except the Local module.

Step 3 Depending on the authentication module you selected, enter the following data, then click **Submit**:.

- Radius module or TACACS+ module:
  - Primary Server and Secondary Server—IP addresses or DNS names of the primary and secondary authentication servers. A secondary server is optional.
  - Shared Secret—Secret key.
- MS NT Domain module:
  - Domain—Name of the Windows domain.
  - Primary Domain Controller and Backup Domain Controller—Names of the primary and backup Windows domain controllers. A backup domain controller is optional.

After you change the authentication module, you do not have to restart the Wireless LAN Solution Engine. Changing the module does not affect users who are currently logged on. Users who log on after the change use the new module.

Related Topic

Overview: Security, page 5-45

Managing SSL (HTTPS)

SSL (secure socket layer) protocol provides a secure connection between Web clients and the Wireless LAN Solution Engine. When you initially set up the Wireless LAN Solution Engine, an unsigned certificate and a CSR (Certificate Signed Request) are automatically generated and SSL is enabled. The unsigned certificate expires in one year. To obtain a permanent, signed certificate, use the following procedure.

Note To establish a connection to the Wireless LAN Solution Engine using SSL, use the prefix https instead of http when entering the URL into the browser and do not append a port number to the URL.

Procedure

Step 1 Select **Administration > Appliance > Security > SSL (HTTPS)**. The SSL (HTTPS) dialog box appears.

Step 2 Click **View CSR**. The encrypted CSR is displayed.

Step 3 Copy the encrypted CSR (between the *begin* and *end* lines). Send the CSR to a certificate authority (such as Verisign), following the authority's procedure.

Step 4 When you receive the signed certificate:

a. Copy it into an ASCII file on a client system.

b. On the same client, select **Administration > Security**.

c. Under SSL (HTTPS), type the path to the signed certificate or click **Browse** to locate the file, then click **Submit Certificate**.

d. To use the new certificate, you need to restart the Wireless LAN Solution Engine by logging on through the CLI, running the **services stop** command to stop the system, then running the **services start** command to restart the system.

Related Topic

Overview: Security, page 5-45

Disabling or Enabling Telnet and Selecting SSH

Telnet is used for connecting to the Wireless LAN Solution Engine through the CLI. By default, Telnet is enabled. To prevent unsecure connections through the CLI, you can disable Telnet.

SSH provides a secure Telnet connection, encrypting all traffic, including passwords. By default, both SSH1 and SSH2 are used.

Procedure

Step 1 Select **Administration > Appliance > Security > SSH and Telnet**. The SSH and Telnet control panel appears.

Step 2 To change the type of SSH used, select the desired SSH version from Select Protocol, then click **Change Protocol**.

Step 3 To enable or disable Telnet, make a selection from Telnet, then click **Configure**.

Changes takes place immediately.

Related Topic

Overview: Security, page 5-45

Viewing the Last 10 Logged-On Users

You can view information about the last 10 users who have logged on to the WLSE.

Procedure

Step 1 Select **Administration > Appliance > Security > Last 10 Logins.**

The Last 10 Logins table appears, showing the following information for the last 10 logins.

Field	Description
Login Name	User's login name.
Logged In Since	Date and time the user logged in (GMT).
IP Address	IP address of the system from which the user logged in.
Associated role	Role assigned to the user.

Related Topic

Overview: Security, page 5-45

Backing Up and Restoring Data

The Backup and Restore options include:

- **Backup**—Back up data, including all Wireless LAN Solution Engine role and user information (see Backing Up Data, page 5-51).
- **Restore**—Restore an available backup image (see Restoring Data, page 5-52).
- **Configure**—Set the backup location (see Configuring the Backup Location, page 5-50).

Configuring the Backup Location

The backup location should be running an FTP server, because the Wireless LAN Solution Engine pushes the backed-up data to the FTP server.

Procedure

Step 1 Select **Administration > Appliance > Backup and Restore > Configure**.

Step 2 Enter the hostname/IP for the backup location.

Step 3 Enter the username you use on the backup location machine.

Step 4 Enter the password you use on the backup location machine.

Step 5 Reenter the password to verify that it is correct.

Step 6 Optional—Specify the path to which the backup image is saved.

Step 7 Click **Save**.

Related Topics

- Backing Up Data, page 5-51
- Restoring Data, page 5-52

Backing Up Data

Data backed up includes Wireless LAN Solution Engine role and user information, seed and discovery (see Managing Device Discovery, page 5-2) configuration information, and customized view information.

Note You should perform a backup every time you add a user, or whenever user views have changed.

Procedure

Step 1 Configure the backup location (see Configuring the Backup Location, page 5-50).

Step 2 Select **Administration > Appliance > Backup and Restore > Backup**.

Step 3 Click **Backup**.

The WLSE saves the backup image.

Step 4 To confirm that your data has been backed up, look at your backup location for a backup directory with saved <*WLSE hostname_date_time*.inf and <*WLSE hostname_date_time*.tar files.

Related Topic

Restoring Data, page 5-52

Restoring Data

Procedure

Step 1 Select **Administration > Appliance > Backup and Restore > Restore**.

Step 2 From the Available Images list, select a backup image. Images are listed by Wireless LAN Solution Engine hostname and date and time of backup.

Step 3 Click **Restore**. The Restore Backup window opens.

Step 4 Click **OK**.

The Wireless LAN Solution Engine shuts down and restarts while data is being restored.

Related Topics

- Backing Up Data, page 5-51
- Configuring the Backup Location, page 5-50

Using Diagnostics

The Diagnostics options are:

- **WLSE Info**—Gather troubleshooting information about the WLSE status and create status reports (see Viewing and Creating a Status Report, page 5-53).
- **Self Test**—Create and display self tests (see Viewing and Creating a Self-Test Report, page 5-53).
- **Processes**—View WLSE processes status, stop and start processes (see Viewing Processes, page 5-54).

Viewing and Creating a Status Report

You can gather troubleshooting information about the status of the Wireless LAN Solution Engine using this option.

Status reports show information about the product database status, product process status, log files, and so on.

Note Status reports reflect the UTC time.

Procedure

Step 1 Select **Administration** > **Appliance** > **Diagnostics** > **WLSE Info**. The WLSE Information and Status Report dialog box appears.

Step 2 To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.

Step 3 To create a new report, click **Create**. It will take five to seven minutes for the report to be complete. To display the new report, click its name. If the new report is not listed, click **Refresh**.

Step 4 To delete a report, click the report check box, then click **Delete**.

Related Topics

- Viewing and Creating a Self-Test Report, page 5-53
- Viewing Processes, page 5-54

Viewing and Creating a Self-Test Report

Self-tests include memory, database, DNS setup, and backup location configuration tests. Self-test reports indicate whether the tests passed or failed.

Note Self-test reports reflect UTC time.

Procedure

Step 1 Select **Administration > Appliance > Diagnostics** > **Self Test**. The WLSE Self-Test Report dialog box appears.

Step 2 To display a report, click its name. If there are no reports listed, you must create a new report by clicking **Create**.

Step 3 To display the new report, click its name. If the report is not displayed, click **Refresh**.

Step 4 To delete a report, select the report check box, then click **Delete**.

Related Topics

- Viewing and Creating a Status Report, page 5-53
- Viewing Processes, page 5-54

Viewing Processes

You can view the status of the major processes running on the Wireless LAN Solution Engine using this option. You can also start and stop processes and access complete reports.

Procedure

Step 1 Select **Administration > Appliance > Diagnostics** > **Processes**. The Process Report displays the following:

Column	Description
Process name	Describes how a process is registered.
State	Process status and a summary of the log file entries for the process.
Pid	Process ID. A unique number by which the operating system identifies each running program.

Column	Description
RC	Return code. “0” represents normal program operation. Any other number typically represents an error. Refer to the error log.
Signo	Signal number. “0” represents normal program operation. Any other number is the last signal delivered to the program before it terminated.
Start Time	Time (UTC) and date the process was started.
Stop Time	Time (UTC) and date the process was stopped.
Core	The entry “Not applicable” means the program is running normally. The entry “Core file created” means the program is not running normally and the operating system has created a file called a core file. The core file stores important data about processes.
Information	The entry indicates what the process is doing. “Not applicable” means the program is not running normally.

Step 2 Perform any or all of these tasks:

- To view details, click any process name. The Daemon Information window opens.
- To view process status, click any process state. The System Log window opens.
- To stop a process, select the check box next to the process name and click **Stop**. The Process Status table displays the new status and other process information. The WebServer and Tomcat processes cannot be stopped.
- To start a stopped process, select the check box next to that process name and click **Start**. The Process Status table displays the new status and other process information.
- To update the Process Status table with the latest data, click **Refresh**. The table does not automatically update.

- To see a complete report of all processes running on the WLSE, click **Complete Report**.

Processes Displayed

The Process Status table displays the status of the following major WLSE-specific processes:

Process Name	Description
WLSEjobvm	The job virtual machine.
WLSEFaults	The fault manager.
WebServer	The Web Server.
Tomcat	The Java servlet engine.
ExcepReporter	The process that forwards traps.
CDPbrdcast	The CDP daemon that identifies Cisco devices to their immediate neighbors.
PerfMon	The process that monitors performance.

Daemon Information

The Daemon Information dialog box displays the following:

Field	Description
Process	The process name.
Path	The file location.
Flags	The flags used to register the process with the Daemon Manager.
Startup	The method used to start the process.
Dependencies	The other processes that must be running for this process to run.

System Log

The system log, which describes the status of the processes running in the system, displays the following:

Field	Description
Timestamp	The date and time the message is logged.
Process	The process that logged the message.
Type	The message type, such as INFO, WARNING, CRITICAL.
Information	The process status as known by the Daemon Manager.

Setting Up the Splash Screen Message

The Splash Screen Message window allows you to set up a message that is displayed when a user logs in. After viewing the message, the user must click **Agree** to continue logging in, or click **Disagree** to log out.

Procedure

Step 1 Select **Administration** > **Appliance** > **Splash Screen**. The Splash Screen Message window appears.

Step 2 Enter the message to be displayed.

Step 3 Check the **Enable** check box, then click **Apply**. The splash screen message is enabled.

Note You *must* check **Enable** for the message to appear.

Managing System Parameters

The System Parameters window allows you to set global parameters. For example, to set the interval at which the Wireless Clients reports will be updated, change the Wireless Client Polling Interval parameters.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > System Parameters**. The following parameters are displayed in the System Parameters window:

Parameter	Description
Inventory Polling Interval	Interval at which the configuration data will be collected from the devices. (This is the data shown in any GUI device detail table.) **Tip** For more accurate trending, set this parameter at a lower interval than Inventory Performance Attributes Polling Interval. Default: 1 hour
Inventory Performance Attributes Polling Interval	Interval at which the performance and utilization data will be collected from the devices. To set the aggregation period of this data, change the Aggregation Interval parameter. Default: 5 minutes
Wireless Client Polling Interval	Interval at which the device data is collected for client information and the Wireless Clients reports are updated. Default: 5 minutes

Parameter	Description
Aggregation Interval	Interval at which the performance data (from Inventory Performance Attributes Polling Interval) is aggregated. (This is the data shown in Report Trends.) **Note** For reports it is necessary to compute some attributes over longer periods (average, percentages, changes). This interval determines how often these computations are performed. Default: 3 hours
Short Term Trending Inventory Truncation Interval	Duration for which the performance data (from Inventory Performance Attributes Polling Interval) is retained by the WLSE. Default: 1 day
Aggregation Truncation Interval	Duration for which the aggregated (historical) data is retained by the WLSE. Default: 15 days
Fault History Truncation Interval	Duration for which the fault data is retained. (This is the data shown in Fault Description.) Default: 30 days
Job History Truncation Interval	Duration for which job data is retained. (This is the data shown in Configure Jobs, Discovery History, Email Jobs.) **Note** Recurring jobs are truncated every day to retain the last 30 runs. Default: 30 days

Step 2 To change any of the parameters, select new values from the pulldown lists and click **Apply** to save the changes. To reset the system parameters to the previous values, click **Reset.**

Note To reset the parameters to previous values, click **Reset** before saving.

A confirmation dialog appears. To return to the System Parameters window, click **Back**.

Administering Users

The User Admin options allow you to manage user roles and logins:

- **Manage Roles**—Add, modify, and delete roles (see Managing Roles, page 5-60).
- **Manage Users**—Add, modify, and delete user accounts (see Managing Users, page 5-62).

Related Topic

Modifying Your Profile, page 5-65

Managing Roles

Use this option to add, modify, and delete user-defined roles and to modify predefined roles. A user's role determines the tabs and subtabs the user can access. Users who have access to a subtab can perform all of the tasks under the subtab.

Although you cannot delete predefined roles, you can modify them. The predefined roles and their default privileges are:

- System administrator—Superuser access to the Wireless LAN Solution Engine (can perform any task). The password is the password assigned during initial WLSE setup (using the console). You can change the password using the console or the WLSE's Manage Users option (see Managing Users, page 5-62).
- Network administrator—Monitoring authority, device configuration authority, and discovery configuration authority.
- Network operator—Monitoring and device configuration authority.
- Help desk—Monitoring authority only.

You can create other roles, which can be modified or deleted.

Note Your login determines whether you can use this option.

Procedure

Step 1 To access the role management window, select **Administration > User Admin > Manage Roles**. Role names are displayed in the center pane. To view the subtabs to which the role has access, select the role.

- The admin user can view all existing roles.
- Other users can only view the roles assigned to them and any roles that they have created.

Step 2 To add a role:

a. Replace the text *New Role* with the name you have chosen for the new role.

b. Select the check boxes next to the features the role will access. Click **Add**.

Note When you select a feature (for example, Display Faults), the role is granted access to the corresponding subtab (for example, **Faults > Display Faults**).

c. The new role appears in the list of roles in the middle pane.

Step 3 To modify a role, select the role. Select the check boxes for the features you want to add to the role and deselect the check boxes next to the features you want to remove from the role. Then click **Modify** to save the changes.

Step 4 To delete a user-defined role, select the role, then click **Delete**.

Related Topics

- Naming Guidelines, page A-1
- Managing Users, page 5-62

Managing Users

Use this option to:

- Add Users, page 5-62
- Modify Users, page 5-63
- Delete Users, page 5-65

Add Users

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > User Admin > Manage Users**. The Add/Modify/Delete dialog appears. The Users list displays the current users.

- The admin user can view and modify all existing users.
- Other users can view their own logins and any users they have created.

Step 2 Enter the following information, in the order shown:

Note To clear your entries and start over, click **Clear**.

Field	Information to Enter
User Name	Enter the name of the new user.
User Password	Enter a password for new user.
Confirm Password	Reenter the password.
Email	Enter the email address of the user (optional).

Field	Information to Enter
CLI Access	Select the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for other users. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset.
Roles	Select one or more roles for the user. To add a role, select it from the pulldown list. To view a role, select it and click **show role**. To remove a role, select it and click **remove**.

Step 3 To add the new user, click **Add**. The new username appears in the Users list. To discard your changes, click **Clear**.

Modify Users

Note Your login determines whether you can use these options.

Procedure

To modify a user:

Step 1 Select **Administration > User Admin > Add/Modify/Delete**. The Add/Modify/Delete dialog appears. The Users list displays the current users.

Note Only the logins created by you are displayed. If logins were created by another user, they are not visible; only their creator can display them. The admin user can view all logins.

Step 2 Select the user from the Users list and make the desired changes:

Field	Information to Enter
User Name	Enter the user's name.
User Password	Enter a new password for new user.
Confirm Password	Reenter the new password.
Email	Enter or change the user's email address.
CLI Access	Change the user's access to the WLSE CLI: None, Level 0, or Level 15. By default, Level 15 is selected for System Administrator, and None is selected for others. Users with privilege level 15 can use all commands, and users with privilege level 0 can use a subset. For information on commands available for each privilege level, see the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*—From the online help, click **View PDF**.
Roles	Change the user's roles. To add a role, select it from the pulldown list. To view a role, select it and click **show role**. To remove a role, select it and click **remove**.

Step 3 Click **Modify** to save your changes or **Clear** to discard your changes.

Related Topics

- Naming Guidelines, page A-1
- Managing Roles, page 5-60

Delete Users

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > User Admin > Manage Users**. The Manage Users dialog appears.

Step 2 Select the username from the Users list, then click **Delete**. A confirmation dialog appears. After you click **OK**, the user is deleted.

Modifying Your Profile

Use the My Profile tab to change your password.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > My Profile > Change password**.

Step 2 To change your password, enter a new password in the New Password and Re-enter New Password fields. For information on allowable characters, see Naming Guidelines, page A-1.

Step 3 Click **Apply** to save your changes or **Reset** to discard your changes.

Related Topic

- Modify Users, page 5-63
- Naming Guidelines, page A-1

Using Connectivity Tools

The options in the Connectivity Tools window allow you to perform connectivity tests and find information about devices.

Note Your login determines whether you can use this option.

Procedure

Step 1 Select **Administration > Connectivity Tools**. The Network Connectivity and Security Test dialog box appears.

Step 2 Enter a device name or IP address in the Device text box.

Step 3 Click an option button:

Note Pressing **Enter** will not work. You *must* click a button.

- Ping—Test device reachability.
- Traceroute—Detect routing errors between the Wireless LAN Solution Engine and the target device.
- NSLookup—Look up device or host information via the name server. The information displayed includes server name, server IP address, device name, and the device IP address.
- TCP Port Scan—Find the active ports on the device.

A results window appears.

Step 4 Click **Close** to close the results window.

CHAPTER 6

Frequently Asked Questions

Q. What ports and protocols does the WLSE use?

A. For discovery and fault monitoring, the WLSE primarily uses SNMP (UDP port 161). For applying configuration changes, the WLSE uses SNMP, HTTP (TCP port 80 or as configured), and TFTP (UDP port 69).

Q. How do configuration files get transferred to access points?

A. Even though access points support both TFTP and FTP, the WLSE uses only TFTP to upload and download configuration files.

Q. Can you undo a configuration update?

A. Yes, but only after a successful configuration update has taken place.

Q. Is Telnet enabled or disabled by default on the WLSE?

A. Telnet is disabled by default for security reasons.

CHAPTER 7

Troubleshooting

This section provides suggestions for troubleshooting the Wireless LAN Solution Engine components. If the suggestions do not resolve the error, check the release notes for a possible work around, or contact the Cisco TAC or your customer support.

This section includes troubleshooting suggestions for the following:

Faults

Feature	Symptom	Probable Cause	Possible Solution
Faults > Display Faults	The Display Fault view is blank.	There are no faults to report based on the filtering criteria you entered.	Not applicable.
Faults > Fault Forwarding	Email fails to arrive at destination.	The SMTP server is not configured properly.	Configure the SMTP server using the **mailroute** command. For information on the mailroute command, select **Help > View PDF**, then select the Command Reference appendix.

Configure

Feature	Symptom	Probable Cause	Possible Solution
Configure > Templates	The access point is inaccessible through the HTTP port set through template configuration job.	The HTTP port setting does not take effect until the access point is cold rebooted.	Cold reboot the access point.
	Template configuration job fails every time.	The access point is not set up properly.	Make sure the WLSE is configured as a TFTP server for the access point. For additional information, see Getting Started, page 1-3.
Configure > Jobs	The Undo function does not work.	Your job is SNMP-based, which is not supported by the Undo function.	None.

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The Undo function does not work.	Your job includes the following Security options, which are not supported by the Undo function: • Local Admin Authentication under the Local Admin Access • Encryption Key Values under Local AP/Client Security • Shared Secret under Server-Based Security. • Shared Secret under Accounting.	None.
		Your job includes the FTP Username and password.	None.
		You are trying to Undo a job that has already been undone.	None.
		Your job is HTTP-based but you have not set up the HTTP credentials.	Add HTTP credentials using **Administration >Discover >Device Credentials > HTTP User/Password**
		You are trying to Undo a job that contains Custom values, which are not supported by the Undo function.	None.

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	HTTP job does not run or fails.	The credentials are not set properly.	Make sure the credentials on the WLSE are the same as the credentials on the access point or bridge using **Administration > Discover > Device Credentials**.
			Make sure the credentials on the access point or bridge have firmware rights.
		The TFTP server is not set up correctly.	The TFTP setting on the access point should point to the WLSE as its TFTP server. This can be done by applying a template configuration, containing TFTP server settings, through an SNMP job (only 11.08T and higher)
	The device is not responding to HTTP jobs.	HTTP browsing is disabled on the AP because of this job run.	At the access point console, turn on non-console browsing, or schedule an SNMP job for the device if its version is11.08T or higher.
	SNMP job does not run or fails.	The community string is not set properly.	Make sure the SNMP community string set on the WLSE is the same as the string set on the access point or bridge using **Administration > Discover > Device Credentials**.
			Make sure the SNMP community string on the access point or bridge has firmware rights.

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job failed.	There are multiple reasons a job may have failed.	Make sure all the bootstrapping steps have been performed correctly on the access point.
			Check the jobvm.log by selecting **Administration > Appliance > Status > View Log File** to further identify and report the problem.
		If after applying a configuration template on a device, the device reboots, the job will be categorized as Failed. When applying a configuration template on a job with multiple devices, if the job fails on even one of the devices, the job is categorized as Failed.	Check if "Verification could not be completed" appears in the **Job Run Detail > Job Run Log** to identify this problem.
	The job is reported as failed, but the configuration was applied successfully to the devices.	The SNMP timeout to the device is too short.	Select **Administration > Discover > Device Credentials > SNMP Communities** and increase the SNMP timeout.

Feature	Symptom	Probable Cause	Possible Solution
Configure > Jobs	The job completed with errors.	This error can be seen in jobs where pre- or post-configuration backups before or after applying the new configuration fail, but the new configuration is applied successfully.	Check if "Completed with errors" appears in the **Job Run Detail > Job Run Log** to identify this problem.
	There is a time discrepancy in scheduled jobs.	The time is not set correctly on the WLSE.	Using CLI commands, reset the time to Universal Coordinated Time (UTC) as follows: 1. Enter **services stop** to stop services. 2. Enter the **clock** command to reset the time. 3. Enter **services start** to restart the services.

Reports

Feature	Symptom	Probable Cause	Possible Solution
Reports	After running a job, the updated data does not appear in a report.	A full polling cycle has not completed and the new data has not been entered in the database.	Verify that the polling cycle has completed as follows: 1. Select **Administration > Appliance > Status > View Log File**. 2. Click **jobvm.log**. 3. Scroll through the log to find the message: "Finished Inventory" for your particular job.
Reports > Scheduled Email Jobs	Email fails to arrive at its destination.	The SMTP server is not configured properly.	Configure the SMTP server using the mailroute command. For information on the mailroute command, select **Help > View PDF**, then, click Command Reference in the table of contents.
	There is a time discrepancy in the scheduled email jobs.	The time is not set correctly on the WLSE.	Using CLI commands, reset the time to Universal Coordinated Time (UTC) as follows: 1. Enter **services stop** to stop services. 2. Enter the **clock** command to reset the time. 3. Enter **services start** to restart the services.

Feature	Symptom	Probable Cause	Possible Solution
Reports > Wireless Clients	The access point data in the Historical Associations report is not accurate.	The wireless client was associated with an access point managed by the WLSE, but it subsequently associated with an access point that was added to the network, but not yet managed by the WLSE.	Verify that the associated access points are in the managed devices folder by selecting Administration > **Discover > Managed Devices > Manage/Unmanage**.
Reports > Current > Summary **Reports > Current > Detailed**	The report for access points is empty.	The SNMP user may not have the correct rights assigned.	Open a browser window to the access point, and select **Setup > Security > User Information**. Make sure that the user corresponding to the SNMP community (which is set up in WLSE in **Discovery > Device Credentials**) has been granted rights for the following: Ident, firmware, admin, snmp, and write. If not, click on the user and assign all these rights.

Administration

Feature	Symptom	Probable Cause	Possible Solution
Administration > Discover > Managed Devices	Devices were discovered but are not displayed in the GUI; for example, in reports.	The devices have not been moved to the Managed state.	Select **Administration > Discover > Managed Devices**. Move the devices from New or Unmanaged to Managed. See Manage Devices, page 5-13.
Administration > Discover > Discover	There is a time discrepancy in the scheduled discovery jobs.	The time is not set correctly on the WLSE.	Using CLI commands, reset the time to Universal Coordinated Time (UTC) as follows: 1. Enter **services stop** to stop services. 2. Enter the **clock** command to reset the time. 3. Enter **services start** to restart the services.
Administration > User Admin > Manage Users	Users are not visible in the list of users.	Only the user who created a given user can view that user's name in the list of users, although the admin user can view all users.	None. For more information, see Managing Users, page 5-62.

Feature	Symptom	Probable Cause	Possible Solution
Administration > **Discover** > **Managed Devices**	Devices were not discovered.	The device is not specified as a seed and the CDP distance is not high enough to reach the device.	Select **Administration** > **Discover** > **Discover** > **Modify Discovery Settings**. Specify the device as a seed or increase the CDP distance. See Add Seed Devices and Schedule Discovery, page 5-10.
		CDP is not enabled on the device.	For more information about device setup, see Set Up Devices, page 5-4. If you are not using CDP, you can import devices from a file or from CiscoWorks2000; see Importing Devices, page 5-21.
		A switch is not discovered unless it has an access point attached to it. Discovery can proceed beyond the switch, but the switch itself is not discovered.	Make sure a properly configured access point is attached to the switch. See Set Up Devices, page 5-4.
		SNMP is not enabled on the device or SNMP community strings are not entered on the WLSE.	SNMP must be enabled on the device and credentials must be entered on the WLSE. See Set Up Devices, page 5-4 or Setting Device Credentials, page 5-17.
		The SNMP timeouts or retries are set too low.	Reset the timeouts and retries. See Setting Device Credentials, page 5-17.
		The device is down.	None.
		The device is not supported.	None.

Naming Guidelines

- **Names and Descriptions**—allowable characters for names and descriptions (see Name and Description Allowable Characters, page A-1).
- **Roles and Users**—rules to follow when creating new roles and users (see Roles and User Rules, page A-2).

Name and Description Allowable Characters

Names—no more than 64 characters allowed

Descriptions—no more than 256 characters allowed

Character Description	Example
alphanumeric—upper and lower case	a123b, A123B
space	
exclamation mark	!
number sign	#
percent sign	%
ampersand	&
left and right parenthesis	( )
asterisk	*
plus sign	+
comma	,
hyphen, dash, minus	-

Character Description	Example
full stop (period)	.
solidus (forward slash)	/
colon	:
semicolon	;
less-than and greater-than signs	< >
equals	=
question mark	?
low line (underscore)	_
left and right square bracket	[ ]
reverse solidus (backward slash)	\
left and right curly bracket	{ }
vertical line	|
tilde	~
dollar sign	$

Roles and User Rules

Type	Rules
User Name	• No more than 32 characters. • Case-sensitive. • Any character from the table above.
User Password	• 5-8 characters. • Case-sensitive. • Any alphanumeric character and an underscore.
Role	• No more than 32 characters. • Case-sensitive. • Any character from the table above.

Command Reference

This appendix summarizes the Wireless LAN Solution Engine's command line interface (CLI) commands. When you make a configuration change using these commands, the system configuration is updated immediately.

This appendix contains the following sections:

Using the CLI

You can use the CLI by:

- Attaching a console to the WLSE
- Accessing the WLSE using Telnet

CLI Conventions

The command-line interface (CLI) uses the following conventions:

- The key combination **^c** or **Ctrl-c** means hold down the **Ctrl** key while you press the **c** key.
- A string is defined as a nonquoted set of characters.

Do not confuse the WLSE's CLI with the IOS CLI. Though they are similar, they are not identical.

Command Privileges

Access to CLI commands is controlled by your user account privilege level. Users with privilege level 15 can use all commands. Users with privilege level 0 can use only a subset of the commands. The command descriptions in this appendix are organized by privilege level. For more information about user accounts and privileges, refer to Administering Users, page 5-60.

Checking Command Syntax

The user interface provides several types of responses to incorrect command entries:

- If you enter a command line that does not contain any valid commands, the system displays `Command not found.`
- If you enter a valid command but omit required options, the system displays `Incomplete command.`

- If you enter a valid command but provide invalid options or parameters, the system displays Invalid input.

In addition, some commands have command-specific error messages that notify you that a command is valid, but that it cannot run correctly.

Command History Feature

The CLI provides a command history feature. To display previously entered commands, press the up arrow key. After pressing the up arrow key, you can press the down arrow key to display the commands in reverse order. To run a command, press the Enter key while the command is displayed on the command line. You can also edit commands before pressing the Enter key.

Help for CLI Commands

You can obtain help using the following methods:

- For a list of all commands and their syntax, type **help** and press **Enter**.
- For help on a specific command, use either of the following methods:
  - Type the command name, a space, **help**; then press **Enter**. For example, **ntp help**.
  - Type **help**, a space, and the command name; then press **Enter**. For example, **help ntp**.

The help contains command usage information and syntax.

Command Summary

Table B-1 summarizes all commands available on the WLSE. Refer to the full description of commands that you are not familiar with before using them.

Table B-1 Command Summary

Command	Privilege Level	Summary Description	Location of Full Description
auth	15	Enables secure remote authentication.	"auth" section on page B-16
backup	15	Backs up the WLSE.	"backup" section on page B-17
backupconfig	15	Sets the configuration for all backup and restore operations.	"backupconfig" section on page B-18
cdp	15	Configures the Cisco Discovery Protocol (CDP).	"cdp" section on page B-19
clock	15	Sets the WLSE's date and time.	"clock" section on page B-20
df	15	Display the current storage usage on the WLSE.	"df" section on page B-22
erase config	15[1]	Erases the configuration in Flash memory and reload the device.	"erase config" section on page B-22
exit	0	Logs user out of the WLSE.	"exit" section on page B-10
gethostbyname	15	Displays IP address of a known domain name.	"gethostbyname" section on page B-24
fsck	N/A[2]	Checks and repairs the filesystem.	"fsck" section on page B-76
firewall		Implements port filtering on the WLSE.	"firewall" section on page B-23
hostname	15	Changes the system hostname.	"hostname" section on page B-25
import	15	Imports host files, or to maps IP addresses to hostnames.	"import" section on page B-25
install configure	15	Configures the repository that the Wireless LAN Solution Engine uses to install updates.	"install configure" section on page B-27

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
install list	15	Lists software updates and images currently available on a configured repository.	"install list" section on page B-28
install update	15	Installs software updates and images from a configured repository.	"install update" section on page B-29
interface	15	Configures an Ethernet interface.	"interface" section on page B-29
ip domain-name	15	Defines a default domain name.	"ip domain-name" section on page B-31
ip name-server	15	Specifies the address of up to three name servers for name and address resolution.	"ip name-server" section on page B-32
listbackup	15	Lists all current backups at the configured site.	"listbackup" section on page B-33
mail	15	Debugs and tests email settings.	"mail" section on page B-34
mailcntrl clear	15	Deletes the maillog, sendqueue, or userqueue.	"mailcntrl clear" section on page B-34
mailcntrl list	15	Lists the size of the userlog, userqueue, or the sendqueue.	"mailcntrl list" section on page B-35
mailroute	15	Forwards email to a specified server.	"mailroute" section on page B-36
nslookup	15	Translates a DNS name to its IP address or an IP address to its DNS name.	"nslookup" section on page B-36
ntp server	15	Configures the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server.	"ntp server" section on page B-37
ping	0	Sends ICMP echo_request packets for diagnosing basic network connectivity.	"ping" section on page B-10
reload	15[1]	Reboots the system.	"reload" section on page B-39
reinitdb	15	Reinitializes the database.	"reinitdb" section on page B-40

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
repository	15	Configures the Wireless LAN Solution Engine to be a repository server.	"repository" section on page B-40
repository add	15	Transfers software updates and images from a remote server to the Wireless LAN Solution Engine's local repository.	"repository add" section on page B-41
repository delete	15	Deletes software updates and images on the Wireless LAN Solution Engine's local repository.	"repository delete" section on page B-42
repository list	15	Lists software updates and images on the configured local or remote repository.	"repository list" section on page B-43
repository server	15	Starts, stops, or displays the status of the Wireless LAN Solution Engine's local repository.	"repository server" section on page B-44
restore	15	Restores a backed up configuration.	"restore" section on page B-45
route	15	Adds a route through a gateway device.	"route" section on page B-46
services	15	Lists, starts, or stops management services.	"services" section on page B-46
show anilog	15	Displays the Wireless LAN Solution Engine's ANI log.	"show anilog" section on page B-48
show auth-cli	15	Displays the type of authentication used for secure CLI access.	"show auth-cli" section on page B-49
show auth-http	15	Displays the type of authentication used for secure HTTP access.	"show auth-http" section on page B-49
show backupconfig	15	Displays the current backup and restore configuration.	"show backupconfig" section on page B-50
show bootlog	0	Displays the messages logged during the last system boot.	"show bootlog" section on page B-51
show cdp neighbor	15	Displays the WLSE's nearest neighbor on the network.,	"show cdp neighbor" section on page B-52

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show cdp run	15	Displays the Cisco Discovery Protocol (CDP) configuration.	"show cdp run" section on page B-52
show clock	0	Displays the system date and time in Coordinated Universal Time (UTC).	"show clock" section on page B-11
show collectorlog	15	Displays the Wireless LAN Solution Engine's collector log.	"show collectorlog" section on page B-53
show config	15	Displays the system configuration.	"show config" section on page B-54
show daemonslog	15	Displays the Wireless LAN Solution Engine's daemons log.	"show daemonslog" section on page B-55
show dmgtdlog	15	Displays the Wireless LAN Solution Engine's daemon manager log.	"show dmgtdlog" section on page B-56
show domain-name	0	Displays the system domain name	"show domain-name" section on page B-12
show hseaccesslog	15	Displays the Wireless LAN Solution Engine's Web access log.	"show hseaccesslog" section on page B-57
show hseerrorlog	15	Displays the Wireless LAN Solution Engine's Web error log.	"show hseerrorlog" section on page B-58
show hsesslaccesslog	15	Displays the Wireless LAN Solution Engine's Web SSL log.	"show hsesslaccesslog" section on page B-59
show import	15	Displays imported host files.	"show import" section on page B-59
show install logs	15	Displays the software updates and images available on the configured repository.	"show install logs" section on page B-60
show interfaces	0	Displays information about the system network interface.	"show interfaces" section on page B-13
show ipchains	15	Displays the IP chains for the selected interface.	"show ipchains" section on page B-60

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
show hosts	15	Displays the Wireless LAN Solution Engine's host file.	"show hosts" section on page B-61
show maillog	15	Displays the Wireless LAN Solution Engine's mail log.	"show maillog" section on page B-62
show process	0	Displays information about processes running on the system.	"show process" section on page B-13
show repository	15	Displays the status or the access log of a configured repository.	"show repository" section on page B-63
show route	15	Displays the routes currently configured.	"show route" section on page B-64
show securitylog	15	Displays the Wireless LAN Solution Engine's secure log information.	"show securitylog" section on page B-64
show snmp-server	15	Displays the Wireless LAN Solution Engine's SNMP configuration.	"show snmp-server" section on page B-66
show ssh-version	15	Displays the type of SSH enabled.	"show ssh-version" section on page B-66
show syslog	15	Displays syslog information.	"show syslog" section on page B-67
show tech	15	Displays information necessary for Cisco's Technical Assistance Center to assist you.	"show tech" section on page B-68
show telnetenable	15	Displays the Wireless LAN Solution Engine's Telnet status.	"show telnetenable" section on page B-68
show tomcatlog	15	Displays the Wireless LAN Solution Engine's Tomcat log.	"show tomcatlog" section on page B-69
show version	0	Displays information about the current software on the system.	"show version" section on page B-14
shutdown	15	Shuts down the system in preparation for powering it off.	"shutdown" section on page B-70

Table B-1 Command Summary (continued)

Command	Privilege Level	Summary Description	Location of Full Description
snmp-server	15	Configures an snmp agent.	"snmp-server" section on page B-71
ssh	15	Connects to an external host using SSH	"ssh" section on page B-71
ssh-version	15	Enables Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.	"ssh-version" section on page B-72
telnet	15	Telnets to an external host.	"telnet" section on page B-72
telnetenable	15	Configures Telnet access.	"telnetenable" section on page B-73
traceroute	0	Displays the network route to a specified host and identify faulty gateways.	"traceroute" section on page B-15
username	15	Creates a new user account or changes an account's properties.	"username" section on page B-74

1. This command is also available in the maintenance image.
2. This command is available only in the maintenance image.

Command Description Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice. Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- Boldface indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

Privilege Level 0 Commands

This section describes the privilege level 0 commands.

exit

To log out of the system, use the exit command.

exit

Syntax Description

This command has no arguments or keywords.

Example

The following command logs you out of the system:

```
exit
```

ping

To send ICMP echo_request packets for diagnosing basic network connectivity, use the **ping** command.

ping [**-c** *count*] [**-i** *wait*] [**-s** *packetsize*] [**-n**] {*hostname* | *ip-address*}

Syntax Description

c	Sets the number of echo packets to send.
count	Number of echo packets to send.
i	Sets the amount of time to wait between sending each packet.
wait	Amount of time to wait between sending each packet, in seconds. The default is 1.
s	Sets the size of each echo packet.
packetsize	The size of each echo packet, in bytes. The default is 56.

hostname	Host name of system to ping.
ip-address	IP address of system to ping.
n	disables reverse DNS lookup.

Usage Guidelines

To use this command with the *hostname* argument, DNS must be configured on the system. To force the time-out of a nonresponsive host or to eliminate a loop cycle, press **Ctrl-c**.

Example

This command sends 4 echo packets to the host otherhost with a wait time of 5 seconds between each packet:

```
ping -c 4 -i 5 209.165.200.224

PING 209.165.200.224 (209.165.200.224) from 209.165.201.0 : 56(84)
bytes of data.
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=0 ttl=246
time=16.3 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=1 ttl=246
time=2.0 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=2 ttl=246
time=2.1 ms
64 bytes from dns-sj1.cisco.com (209.165.200.224): icmp_seq=3 ttl=246
time=2.1 ms
```

show clock

To display the system date and time in Coordinated Universal Time (UTC), use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **show clock** command to display the system date and time. For more information about the system time, see the section "Setting System Date and Time" in the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command displays the system date and time:

```
show clock
12:43:47 Jun 20 2001
```

Related Commands

clock

ntp server

show domain-name

To display the system domain name, use the **show domain-name** command.

show domain-name

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system domain name:

```
show domain-name
cisco.com
```

show interfaces

To display information about the system network interface, use the **show interfaces** command.

show interfaces

Syntax Description

This command has no arguments or keywords.

Example

This command displays information about system network interfaces:

```
show interfaces
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.0
           Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:80309 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22451 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0xef00 Memory:d0c7e000-d0c7ec40
```

Related Commands

interface

show process

To display information about processes running on the system, use the **show process** command.

show process [**page**]

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays information about processes running on the system:

```
show process page
PID  PPID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1     0  4-20:04:35   277 Fri Jun 15 16:54:03 2001 ?    init
    2     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kflushd
    3     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kupdate
    4     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kpiod
    5     1  4-20:04:35     0 Fri Jun 15 16:54:03 2001 ?    kswapd
    6     1  4-20:04:28     0 Fri Jun 15 16:54:10 2001 ?    kreiserfsd
   81     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   82     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   83     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   84     1  4-20:04:25     0 Fri Jun 15 16:54:13 2001 ?    kreiserfsd
   85     1  4-20:04:24     0 Fri Jun 15 16:54:14 2001 ?    kreiserfsd
  199     1  4-20:04:23   290 Fri Jun 15 16:54:15 2001 ?    watchdog
  213     1  4-20:04:23   342 Fri Jun 15 16:54:15 2001 ?    idled
  402     1  4-20:04:17   290 Fri Jun 15 16:54:21 2001 ?    syslogd
  411     1  4-20:04:17   360 Fri Jun 15 16:54:21 2001 ?    klogd
  517     1  4-20:04:15   327 Fri Jun 15 16:54:23 2001 ?    crond
  531     1  4-20:04:15   286 Fri Jun 15 16:54:23 2001 ?    inetd
  540     1  4-20:04:14   585 Fri Jun 15 16:54:24 2001 ?    sshd
  585     1  4-20:04:09   842 Fri Jun 15 16:54:29 2001 ?    dmgtd.lnx
-----------more-----------
```

show version

To display information about the current software on the system, use the **show version** command.

show version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the current software on the system:

```
show version
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
```

```
Uptime: 4 days 20 hours 6 mins
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
```

traceroute

To display the network route to a specified host and identify faulty gateways, use the **traceroute** command.

traceroute [-f *first_ttl***] [-m** *max_ttl***] [-w** *waittime***]** *host* **[***packetlength***]**

Syntax Description

-f	(Optional) Sets the time-to-live used in the first outgoing probe packet.
first_ttl	Time-to-live value of the first outgoing probe packet. The default is 1 hop.
-m	(Optional) Sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets.
max_ttl	Maximum time-to-live for outgoing probe packets. The default is 30 hops.
-w	(Optional) Sets the time to wait for a response to a probe, in seconds.
waittime	Time to wait for a response to a probe, in seconds. The default is 5.
host	Name or IP address of host to which to connect.
packetlength	(Optional) The length of the packet to send, in bytes. The default and minimum value is 40.

Usage Guidelines

Use the **traceroute** command to trace the network route to a specified host and identify faulty gateways. The command displays a list of the hosts that receive probe packets as they travel to the destination host, in the order that the receiving hosts receive the packets. Asterisks (*) appear as the list entry for hosts that do not respond to probing correctly.

Example

This command displays the network route to the host otherhost with a packet time-to-live value of 2, a wait time of 5 seconds, and 50-byte packets:

```
traceroute -m 20 -w 10 cisco.com 50
traceroute to example.com (209.165.200.224), 20 hops max, 50 byte
packets
 1  ex1.com (209.165.200.225)  0.981 ms  0.919 ms  0.926 ms
 2  ex2.com (209.165.200.254)  1.528 ms  0.747 ms 0.661 ms
 3  ex3.com (209.165.200.255)  0.887 ms  0.770 ms  0.744 ms
 4  ex4.com (209.165.201.0)  0.932 ms  0.789 ms  0.679 ms
 5  ex5.com (209.165.201.1)  1.066 ms  1.052 ms  0.983 ms
 6  ex6.com (209.165.201.30)  1.472 ms  1.247 ms  1.847 ms
 7  ex7.com(209.165.201.31)  1.738 ms  1.424 ms  1.658 ms
 8  ex8.com (209.165.202.128)  3.728 ms  2.429 ms  2.804 ms
 9  ex9.com (209.165.202.129)  6.283 ms  5.499 ms 3.285 ms
10  ex10.com (209.165.202.158)  9.926 ms  73.463 ms  3.895 ms
11  ex11.com (209.165.202.159)  70.967 ms *  47.106 ms
```

Related Commands

ping

Privilege Level 15 Commands

This section describes the privilege level 15 commands. Only users with privilege level 15 can run them.

auth

Use the **auth** command to enable secure remote authentication.

auth {cli | http} {local | tacacs *secret server1* **[***server2***] | radius** *secret server1* **[***server2***] | nt** *domain pdc* **[***bdc***]}**

Syntax Description

cli	Enables authentication using the Command Line Interface (CLI).

http	Enables authentication using Hypertext Transfer Protocol (HTTP).
local	Enables local authentication.
tacacs	Enables authentication using the Terminal Access Controller Access Control System (TACACS).
radius	Enables authentication using Remote Dial-In User Service (RADIUS).
nt	Enables authentication from an NT domain controller.
secret	Shared secret code of server.
server1	IP address or DNS name of server from which authentication will occur.
server2	IP address or DNS name of optional secondary server from which authentication could occur
domain	NT domain name.
pdc	Name of the Primary Domain Controller (PDC).
bdc	Name of the Backup Domain Controller (BDC).

Example

This command enables secure remote authentication from a remote server, using TACACS.

```
auth http tacacs tr5e43 209.165.200.224
```

backup

Use the **backup** command to back upthe WLSE.

backup [test]

Syntax Description

test	Tests the configured backup hostname, username, password, and directory.

Usage Guidelines

To back up the WLSE, use the **backup** command. To configure the backup location, use the **backupconfig** command.

Example

The following command backs up the WLSE:

```
backup
```

Related Commands

backupconfig

listbackup

restore

show backupconfig

backupconfig

Use the **backupconfig** command to set the configuration for all backup and restore operations. To clear the backup and restore configuration information, use the **no backupconfig** command.

backupconfig {*hostname***} {***username***} {***password***} [***directory***]**

no backupconfig

Syntax Description

hostname	Host name or IP address of the host system.
username	Username of host system.
password	Password of the host system.
directory	Path to specific backup directory, if different from user's default directory.

Usage guidelines

To set the configuration for all backup and restore operations, use the **backup** command.

Example

The following command will configure the backup and restore operations to backup to and restore from host 209.165.200.224, set the username to user1, and set the password to pass:

```
backupconfig 209.165.200.224 user1 pass
```

The following command clears all backup and restore configuration information:

```
no backupconfig
```

Related Commands

backup

listbackup

restore

show backupconfig

cdp

Use the **cdp** command to configure the Cisco Discovery Protocol

cdp {run [*port***] | timer** *seconds* **| holdtime** *seconds***}**

no cdp {run [*port***] | timer | holdtime}**

Syntax Description

run	start cdp
timer	set cdp packets retransmission time.
holdtime	set cdp packet info hold time.
port	Ethernet port on which CDP will be enabled. Acceptable values are eth0-15.

seconds	amount of time, in seconds, that the system takes to either transmit the cdp packet information or to hold another system's cdp packet information.

Usage Guidelines

Cisco Discovery Protocol (CDP) is a protocol by which one Cisco device can recognize, and be recognized by, another Cisco device. The run command starts the system sending out signals to the other systems. The timer command sets the amount of time, in seconds, that these signals are sent. The holdtime sets the amount of time a system will recognize another system without receiving a signal. For example, if your system's holdtime is set to 30 seconds, and another system that has already been recognized by yours does not send a signal within that 30 seconds, your system will cease to recognize it. If you are using the **no cdp** command, the timer and holdtime commands set their respective values to the default value.

Example

This command sets the cdp packet's retransmission time at 10 seconds.

```
cdp timer 10
```

This command sets the cdp packet's retransmission to its default time.

```
no cdp timer
```

clock

To set the system date and time, use the **clock** command. See the Usage Guidelines before using this command.

clock {set *hh***:***mm***:***ss month day year***}**

Syntax Description

set	Sets the system clock.
*hh***:***mm***:***ss*	Current time (for example, 13:32:00).

month	Current month. You can enter full month names or abbreviations that include at least the first 3 characters of the month name (for example, jan, feb, mar).
day	Day of the month (for example, 1 to 31).
year	Current year (for example, 2000).

Usage Guidelines

When resetting the time, you must stop and restart WLSE services:

Step 1 Stop services:

```
services stop
```

Step 2 Change the time.

Step 3 Start services:

```
services start
```

To set the date and time, use the **set** option.

If you configure the system to use Network Time Protocol (NTP), you do not need to set the system clock manually using the **clock** command.When setting the clock, enter the current time in Coordinated Universal Time (UTC).

For more information about the system time, refer to "Setting System Date and Time" in the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command sets the date and time:

```
clock set 16:00:00 dec 11 2001
```

```
Tue Dec 11 16:00:00 UTC 2001
```

Related Commands

ntp server

show clock

df

To display the current storage usage on the WLSE, use the **df** command.

df

Usage Guidelines

This command in primarily intended as a debugging tool for problems with full partitions.

Example

The following command displays the current storage usage on the WLSE:

```
df
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda12            151M   59M   92M  39% /
/dev/sda1              49M  2.8M   44M   6% /boot
/dev/sda7             985M   24M  911M   3% /extra
/dev/sda8             601M   32M  569M   5% /home
/dev/sda6            1001M  136M  865M  14% /opt
/dev/sda13            9.7G   32M  9.7G   0% /tftpboot
/dev/sda9             601M   32M  569M   5% /tmp
/dev/sda10            591M  212M  350M  38% /usr
/dev/sda5             2.9G  450M  2.5G  15% /var
```

erase config

To erase the configuration in flash memory and reload the device, use the **erase config** command.

erase config

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to erase the configuration in Flash memory and reload the device.

When you enter the command, you are prompted for confirmation. Enter **yes** to confirm, or press **Enter** to accept the default response **no**.

Caution When you confirm this command, the system configuration is erased and the system reboots automatically. The system will not operate until you reconfigure it.

When the system reboots, you must reconfigure it with the setup program. For information about using the setup program, refer to the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

Example

This command erases the system configuration:

```
erase config
This will erase your configuration, return device t
o factory defaults, and reload the device
Do you want to continue?[no]:yes
```

firewall

To implement port filtering on the WLSE, use the **firewall** command.

firewall *eth <0-5>* **[public | private] | [icmp telnet ssh snmp https 1741]**

Syntax Description

eth <0-5>	Port to be configured. Acceptable values are eth0-5.
public	Denies access via ICMP, Telnet, SNMP, and the HTTP 1741 port.
private	Denies no access.
icmp	Denies Internet Control Message Protocol (ICMP) ping messages.

telnet	Denies incoming Telnet connections.
ssh	Denies incoming SSH connections.
snmp	Denies incoming SNMP requests.
https	Denies all connections to the SSL HTTP port.
1741	Denies all connections to the HTTP 1741 port.

Usage Guidelines

Use the firewall command to implement port filtering on the WLSE. To configure an Ethernet port for secured public access, use the **public** option. To configure an Ethernet port for local access, via a LAN or VLAN, use the **private** option. To *dissable* icmp, Telnet, ssh, snmp, https, or to deny connections to the SSL HTTP port or the HTTP 1741 port, use its corresponding option.

Example

The following is an example of a secure Ethernet port configuration:

- The Ethernet 0 port is connected to the Internet, and is configured to be accessible only via HTTPS by entering the following command:

  ```
  firewall eth0 public ssh 1741
  ```

- The Ethernet 1 port is connected to an internal LAN or VLAN, and is configured to be accessible via any of the supported protocols by entering the following command:

  ```
  firewall eth1 private
  ```

  An on-site user has full access to the WLSE, but an external user can only access it using a secure connection.

gethostbyname

Use the gethostbyname command to display the IP address of a known domain name.

gethostbyname *host*

Syntax Description

host	Domain name of host.

Example

This command displays the IP address of example.com

```
gethostbyname example.com
209.165.200.224
```

hostname

To change the system hostname, use the **hostname** command.

hostname *name*

Syntax Description

name	New hostname for the WLSE; the name is case sensitive and may be from 1 to 22 alphanumeric characters.

Example

The following example changes the hostname to sandbox:

```
hostname sandbox
```

import

To import host files, or to map IP addresses to hostnames, use the **import** command:

import {host *hostname ipaddress***} | {hosts** *ftp-host username password path***}**

no import {host *hostname ipaddress***} | {hosts}**

Syntax Description

host	Maps one IP address to a hostname.
hostname	Hostname to map IP address to.
hosts	Imports host files from ftp accessible host.
ipaddress	IP address to map Hostname to.
password	Password used to access ftp accessible host.
path	Path to ftp accessible host.
ftp-host	IP address of ftp accessible host.
username	username use to access ftp accessible host.

Usage Guidelines

To map a single hostname to an IP address, enter the import command as follows

import host *hostname ipaddress*

To import host files from an external, ftp accessible server, enter the import command as follows:

import hosts *ftp-host username password path*

To remove an individual IP address from a host file, use the **no** version of the **import** command as follows:

no import host *hostname ipaddress*

To remove an imported host file, use the **no** version of the **import** command as follows:

no import hosts

Example

This command imports host files from the ftp accessible server ftpserver_1. Ftpserver_1 has the username admin, the password pass, and the path /ftpserver_1/hosts.

```
import hosts ftpserver_1 admin pass /ftpserver_1/hosts
```

This command deletes the hosts imported in the example above:

```
no import hosts
```

install configure

To define the repository that the Wireless LAN Solution Engine uses to install software updates and images, use the **install configur**e command.

install configure {URL *URL Value* **| default | save}**

Syntax Description

URL	Sets the URL of the repository.
URL Value	The URL of the repository. The URL should take the form of http://host:port/path (the path is not a requirement).
default	Configures the Wireless LAN Solution Engine to be its own repository. The URL is http://localhost:9851.
save	Saves the current configuration in the install.ini file.

Usage Guidelines

The **install configure** command defines the repository that the Wireless LAN Solution Engine uses. A repository is a remote or local server from where a system can download software updates and images. Only HTTP is supported.

Example

The following command configures the Wireless LAN Solution Engine to use http://209.165.200.22, with port 9851, as a repository:

```
install configure URL http://209.165.200.224:9851
```

Related Commands

install update

install list

install list

To list software updates and images currently available on the configured repository, use the **install list** command.

install list [all | full | page | updates]

Syntax Description

all	Displays all software updates and images on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the software.
full	Displays only the complete images on a configured repository.This command displays the name, the version, the requirements, the type, and a summary of the image.
page	Displays only the names of all software updates and images on a configured repository. All other information is omitted.
updates	Displays only the updates on a configured repository. This command displays the name, the version, the requirements, the type, and a summary of the update.

Usage Guidelines

The **install list** command displays software updates and images currently available on a repository. A repository is a remote or local server from where a system can receive software.

Example

Enter the following command to display a list of all available software updates and images on a configured repository:

```
install list all
Name            Version Requires        Type       Summary
 EX-1.02        1.02    HSE-1.0         UPDATE     Hosting Solution...
 EX-1.1aR       1.1aR   HSE-1.1         UPDATE     Hosting Solution...
 EX-1.1a        1.1a    HSE-1.1         UPDATE     Hosting Solution...
 EX-1.0a        1.0a    HSE-1.0         UPDATE     Hosting Solution...
 EX-1.0aR       1.0aR   HSE-1.0         UPDATE     Hosting Solution...
 EX-1.0-ROB     1.0     HSE-1.0         COMPLETE   Hosting Solution...
 EX-1.0         1.0     HSE-1.0         COMPLETE   Hosting Solution...
```

Related Commands

install configure

install update

install update

To install a software update or image, use the **install update** command.

install update *package name*

Syntax Description

Package Name	Name of the software update or image to be installed. To see the names of software updates and images available for installation, use the **install list** command. For more information, see the "install list" section on page B-28.

Example

The following command installs the update EX-2.0:

```
install update EX-2.0
```

Related Commands

install configure

install list

interface

To configure an Ethernet interface, use the **interface** command.

interface *eth<0-5>* **{[up | down] |** *ipaddress netmask* **[default-gateway** *address***] [up | down]}**

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.
up	Enables the interface (the default). If you include the *ipaddress* parameter and want to enable the interface in the same command, either enter the **up** parameter after *ipaddress* and its required parameters, or do not specify the **up** or **down** parameters (**up** is the default).
down	Disables the interface. If you include the *ipaddress* parameter and want to disable the interface in the same command, enter the **down** parameter after *ipaddress* and its required parameters.
ipaddress	The IP address of the interface.
netmask	The netmask of the interface IP address.
default-gateway	Changes the IP address of the default gateway that connects the WLSE to the network.
address	The gateway IP address.

Default

When you enter the **interface** command, the interface that you specify is enabled by default. If you want to disable an enabled interface or leave a disabled interface disabled, you must specify the **down** option.

Usage Guidelines

Use the **interface** command to configure an Ethernet interface.

If you change the IP address or hostname, follow these steps to ensure that applications using the system can connect to it correctly:

Step 1 Stop and restart management services by entering:

```
# services stop
```

```
# services start
```

Step 2 Verify that management applications that use the system can still connect to it.

Step 3 Reconnect any applications that cannot connect to it using the system's new IP address or hostname.

Example

This command disables the Ethernet 1 interface:

```
interface eth1 down
```

This command sets the Ethernet 0 IP address, netmask, and gateway IP address:

```
interface eth0 209.165.200.224 255.255.255.224 default-gateway
209.165.201.31 up
```

ip domain-name

To define a default domain name, use the **ip domain-name** command. To remove the default domain name, use the **no** form of the command.

ip domain-name *name*

no ip domain-name *name*

Syntax Description

name	Domain name (e.g. cisco.com).

Usage Guidelines

Use this command to define a default domain name.

A default domain name allows the system to resolve any unqualified host names. Any IP hostname that does not contain a domain name will have the configured domain name appended to it. If you are using a DNS server, this appended name is resolved by the DNS server, and then added to the host table.

Example

This command defines the default domain name cisco.com:

```
ip domain-name cisco.com
```

This command removes the default domain name:

```
no ip domain-name
```

Related Commands

ip name-server

ip name-server

To specify the address of up to three name servers for name and address resolution, use the **ip name-server** command. To disable a name server, use the **no** form of the command.

ip name-server *ip-address*

no ip name-server *ip-address*

Syntax Description

ip-address	Name server IP address (maximum of 3).

Usage Guidelines

Use the **ip name-server** command to point the system to a specific DNS server. You may configure up to three servers.

If you attempt to configure a fourth name server, the following error message appears:

```
# Name-server table is full.
```

The system must have a functional DNS server configured to function correctly. If it does not, in most cases it will not correctly process requests from management applications that use it. If the system cannot obtain DNS services from the network, Telnet connections to the system will fail or Telnet interaction with the system will become extremely slow.

Example

This command assigns a name server for the system to use for DNS name to address resolution:

```
ip name-server 209.165.200.224
```

This command disables the name server; the system will not use it for name to address resolution:

```
no ip name-server 209.165.200.224
```

Related Commands

ip domain-name

listbackup

Use the **listbackup** command to list all current backups at the configured site.

listbackup

Syntax Description

This command has no arguments or keywords.

Example

The following command lists all current backups at the configured site:

```
listbackup
ex1_06042001_170640: Hostname: ex1 Date: 06042001  time: 1700
ex1_06052001_124543: Hostname: ex1 Date: 06052001  time: 1243
ex1_06052001_155148: Hostname: ex1 Date: 06052001  time: 1558
ex1_06202001_145704: Hostname: ex1 Date: 06202001  time: 1454
```

Related Commands

backup

backupconfig

restore

show backupconfig

mail

To debug and test email settings, use the **mail** command.

mail [to *user@host* **[debug]]**

Usage Guidelines

Entering the **mail** command with no arguments will allow you to read email. Entering the **mail** command with the arguments listed will allow you to send email.

Syntax Description

to	Sends email to the expressed recipient.
user@host	Recipient of the email.
debug	Debugs any email problems.

Example

The following command sends an email message:

```
mail to johndoe@example.com
```

mailcntrl clear

To delete the maillog, sendqueue, or userqueue, use the **mailcntrl clear** command.

mailcntrl clear {log | sendqueue | userqueue}

Syntax Description

log	Clears the WLSE's email log.
sendqueue	Clears the WLSE's sendqueue.
userqueue	Clears the WLSE's userqueue.

Example

The following command clears the WLSE's email log.

```
mailcntrl clear log
```

Related Commands

mailcntrl list

mailcntrl list

To list the size of the userlog, userqueue, or the sendqueue, use the **mailcntrl list** command.

mailcntrl list {logsize | sendqueuesize | userqueuesize}

Syntax Description

logsize	Size of the mail log.
sendqueuesize	Size of the sendqueue.
userqueuesize	Size of the userqueue.

Example

The following command displays the size of the WLSE's email log.

```
mailcntrl list logsize
Mail log files total size: 4.0k
```

Related Commands

mailcntrl clear

mailroute

To forward email to a specified SMPT server, use the **mailroute** command. If no server is specified, the WLSE will use DNS to resolve the correct email server in your local domain.

mailroute {*hostname* **|** *ip-address***}**

Syntax Description

hostname	Host name of an email server.
ip-address	IP address of an email server.

Example

The following command forwards email to a server with the hostname mailserver:

```
mailroute mailserver
```

nslookup

To translate a DNS name to its IP address or an IP address to its DNS name, use the **nslookup** command.

nslookup {*dns-name* **|** *ip-address***}**

Syntax Description

dns-name	DNS name of a host on the network.
ip-address	IP address of a host on the network.

Example

The following command translates the DNS name hostname to its IP address:

```
nslookup hostname
Server: dns.ex1.com
Address: 209.165.200.224

Name:    ex1.com
Address: 209.165.201.0
```

ntp server

To configure the Network Time Protocol (NTP) and allow the system clock to be synchronized by a time server, use the **ntp server** command. To disable this function, use the **no** form of this command.

ntp server *ip-address*

no ntp server *ip-address*

Syntax Description

ip-address	IP address of the NTP time server providing clock synchronization.

Usage Guidelines

Use the **ntp server** command to synchronize the system clock with the specified NTP server. If you configure multiple NTP servers, the system will synchronize with the first working NTP server it finds. There is no limit to the number of NTP servers that you can configure.

The **ntp server** command validates the NTP server that you specify. The possible results are:

- If the server is a valid NTP server, a message similar to the following appears:

  ```
  # 19 Jan 00:43:48 ntpdate[1437]: step time server 209.165.200.224
  offset 999.257304
  ```

- If no NTP server with the name or IP address you specified exists, a message similar to the following appears:

  ```
  # 19 Jan 00:43:40 ntpdate[1431]: no server suitable for
  synchronization found
  ```

  In this case, remove the NTP server by using the **no** form of the command, then configure a valid NTP server.

- If the system time is set to a time later than the time on the NTP server, a message similar to the following appears:

  ```
  # 19 Jan 00:43:58 ntpdate[1265]: Can’t adjust the time of day:
  Invalid argument.
  ```

In this case, the **ntp server** command is entered into the system configuration, but NTP will not function. Follow these steps to remove the command and configure NTP correctly:

Step 1 Remove the **ntp server** command from the configuration by entering the **no** form of the command. For example:

`no ntp server` *ip-address*

where *ip-address* is the IP address of the NTP server.

Step 2 Set the system clock to a time that is behind the time on the NTP server using the **clock set** command. For more information about the clock command, refer to the "clock" section on page B-20.

Step 3 Enter the **ntp server** command again to configure the NTP server on the system. For example:

`ntp server` *ip-address*

Example

This command configures the system to use an NTP server:

```
ntp server 209.165.201.0
```

This command configures the system to stop using the NTP server:

```
no ntp server 209.165.201.0
```

Related Commands

clock

reload

To reboot the system, use the **reload** command.

reload

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **reload** command to reboot the system.

You are prompted to verify the reload. Enter **yes** to confirm or **no** to cancel the reload.

Caution All processes running on the system stop when you run the reload command. The WLSE will not respond while it is reloading.

Example

This command reboots the system:

```
reload
```

Related Commands

shutdown

reinitdb

To reinitialize the database, use the **reinitdb** command.

reinitdb

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

The **reinitdb** command reinitializes the database. This erases all information contained within the database.

Example

This command reinitializes the database:

```
reinitdb
```

repository

To configure the Wireless LAN Solution Engine to be a repository server, use the **repository** command.

repository source *URL*

Syntax Description

source	Sets the location from where the local repository downloads software updates and images.
URL	The IP address of an external server containing software updates and images.

Usage Guidelines

The **repository** command allows the Wireless LAN Solution Engine to be a repository both for itself and for external systems. A repository is a remote or local server from where a system can receive software updates and images.

The **repository** command only configures the Wireless LAN Solution Engine to be a repository. To configure the Wireless LAN Solution Engine to install software updates and images from this repository, see the "install configure" section on page B-27.

Example

To configure the Wireless LAN Solution Engine to be a repository, and to download software updates and images from http:// 209.165.200.224, enter the following command:

```
repository source ftp://209.165.200.224
```

Related Commands

repository add

repository delete

repository list

repository server

repository add

To transfer software updates and images from a remote server to the Wireless LAN Solution Engine's local repository, use the **repository add** command.

repository add *package*

Syntax Description

package	Name of the software update or image to be transferred.

Usage Guidelines

The **repository add** command transfers software updates and images from a remote server to the Wireless LAN Solution Engine's local repository. You will be prompted to enter a username and password if they are needed to access the remote server.

Example

To transfer the update EX_2.0 from an update server to the local repository, enter the following command:

```
repository add ex_2.0
```

Related Commands

repository

repository delete

repository list

repository server

repository delete

To delete software updates and images on the Wireless LAN Solution Engine's local repository, use the **repository delete** command.

repository delete [*package* **| all]**

Syntax Description

all	Deletes all software updates and images in the local repository.
package	Name of the software update or image to be deleted.

Usage Guidelines

The **repository delete** command deletes software updates and images on the Wireless LAN Solution Engine's local repository. A repository is a remote or local server from where a system can receive software updates and images.

Example

The following command deletes the update EX_2.0 from the local repository:

```
repository delete EX_2.0
```

Related Commands

repository

repository add

repository list

repository server

repository list

To list software updates and images on the configured local or remote repository, use the **repository list** command.

repository list {local | remote} [detail] [page]

Syntax Description

local	Lists software updates and packages on the local repository.
remote	Lists software updates and packages on a remote repository.
detail	Includes details of the software updates and images displayed.
page	Displays the software updates and packages on page at a time.

Example

To list the software updates and images available on the configured local repository, with details and one page at a time, enter the following command:

```
repository list local detail page
```

Related Commands

repository

repository add

repository delete

repository server

repository server

To start, stop, or view the status of the Wireless LAN Solution Engine's local repository, use the **repository server** command.

repository server [stop | start | status]

Syntax Description

stop	Stops the local repository.
start	Starts the local repository.
Status	Displays the status of the local repository.

Usage Guidelines

The **repository server** command starts, stops, or displays the status of the Wireless LAN Solution Engine's local repository. A repository is a remote or local server from where a system can receive software updates and images.

Example

The following command stops the local repository:

```
repository server stop
```

Related Commands

repository

repository add

repository delete

repository list

restore

Use the **restore** command to restore a backed up configuration of the WLSE.

restore *restore name*

Syntax Description

restore name	Name of backup to be used to restore the WLSE.

Usage Guidelines

To restore a configuration, use the **restore** command. If you use the **restore** command all current domains, roles, users, and discovery configuration information will be erased.

Example

The following command will restore a backed up configuration:

```
restore backup1
```

Releated Commands

backup

backupconfig

listbackup

show backupconfig

route

To add a route through a gateway device, use the **route** command. To delete a route, use the no version of the command.

route {*network address***} netmask {***network netmask***} gateway {***gateway address***}**

no route {*network address***} netmask {***network netmask***}**

Syntax Description

netmask	Sets value of the network netmask.
gateway	Sets the IP address of the router or gateway.
network address	IP address of the network.
network netmask	Value of the network netmask.
gateway address	IP address of router or gateway.

Example

The following command adds a route:

```
route 209.165.201.0 netmask 255.255.255.224 gateway 209.165.200.224
```

The following command deletes the above route:

```
no route 209.165.201.0 netmask 255.255.255.224
```

services

To list, start, or stop the management services running on the system, use the **services** command.

services [status | start | stop]

Syntax Description

status	Displays the management services status.
start	Starts the management services.
stop	Stops the management services.

Usage Guidelines

Use this command to start, stop, or view status of the management services running on the system.

Management services are the software installed on the system by network management applications. Use this command to stop and restart the management services if the system is not responding correctly to a management application. This should cause the services to reset and function properly again.

Example

This command stops management services:

```
services stop
```

This command starts management services:

```
services start
```

This command shows services status:

```
# services status
Process= HSECollector
        State  = Running but busy flag set
        Pid    = 588
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
        Stop   = Not applicable
        Core   = Not applicable
        Info   = HSECollector started.

        Process= HSEANIServer
        State  = Running but busy flag set
        Pid    = 589
        RC     = 0
        Signo  = 0
        Start  = 06/15/01 16:54:32
-----------more-----------
```

Related Commands

show process

show anilog

To display the Wireless LAN Solution Engine's ANI log, use the **show anilog** command.

show anilog [page] | include *MatchString1* **[***MatchString2***]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's ANI log, one page at a time:

```
show anilog page
/var/adm/CSCOets/log/ani.log
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
n=15, max=48, maxIdleSecs=240
2001/12/20 13:43:12 main ani MESSAGE DBConnection: Created new
Database connecti
on [hashCode = 45981573]
2001/12/20 13:43:38 main ani MESSAGE ServletServiceModule: Moxie
Servlet Engine
is ready to receive requests
2001/12/20 15:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 85057415]
```

```
2001/12/20 17:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
 connection [hashCode = 396959623]
2001/12/20 19:43:39 HSEStatusPoll ani MESSAGE DBConnection: Created
new Database
--More--
```

show auth-cli

To display the type of authentication used for secure CLI access, use the **show auth-cli** command.

show auth-cli

Syntax Description

This command has no arguments or keywords.

Example

This command and response shows that the WLSE's local authentication is being used for the CLI:

```
show auth-cli
local
```

show auth-http

To display the type of authentication used for secure HTTP access, use the **show auth-http** command.

show auth-http

Syntax Description

This command has no arguments or keywords.

Example

This command and response shows that the WLSE's local authentication is being used for the CLI:

```
show auth-http
local
```

show backupconfig

The **show backupconfig** command displays the current backup and restore configuration.

```
show backupconfig
```

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

To display the current backup and restore configuration, use the **show backupconfig** command. If the backup configuration has not been set, the host and username fields display NONE.

Example

The following command displays the current backup and restore configuration:

```
show backupconfig
Hostname: 209.165.201.0
Username: user1
```

Related Commands

backup

backupconfig

listbackup

restore

show bootlog

To display the messages logged during the last system boot, use the **show bootlog** command.

show bootlog [page]

Syntax Description

page	Displays command output one screen at a time. Press the **return** key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays the messages logged during the last system boot:

```
show bootlog page
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Console: colour VGA+ 80x25
Calibrating delay loop... 1133.77 BogoMIPS
start low memory: 0xc0001000 i386_endbase: 0xc009f000
addresses range:: 0xc0f00000  0xc1000000
start memory: c04f8000 end_memory: d0000000
Memory: 257688k/262144k available (988k kernel code, 416k reserved,
2992k data,)
Dentry hash table entries: 262144 (order 9, 2048k)
Buffer cache hash table entries: 262144 (order 8, 1024k)
Page cache hash table entries: 65536 (order 6, 256k)
vmdump: setting dump_execute() as dump_function_ptr ...
VFS: Diskquotas version dquot_6.4.0 initialized
CPU: Intel Pentium III (Coppermine) stepping 06
Checking 386/387 coupling... OK, FPU using exception 16 error
reporting.
Checking 'hlt' instruction... OK.
POSIX conformance testing by UNIFIX
mtrr: v1.35a (19990819) Richard Gooch (rgooch@atnf.csiro.au)
PCI: PCI BIOS revision 2.10 entry at 0xfda95
PCI: Using configuration type 1
-----------more-----------
```

Related Commands

reload

clock

show cdp neighbor

To display the WLSE's nearest neighbor on the network, use the **show cdp neighbor** command.

show cdp neighbor

Syntax Description

This command has no arguments or keywords.

Example

This command shows the nearest neighbor on the network.

```
show cdp neighbor
cdp neighbor device: Switch
        device type: cisco WS-C2924-XL
        port: FastEthernet0/12
        address: 209.165.201.0
```

show cdp run

To display the Cisco Discovery Protocol (CDP) configuration, use the **show cdp-run** command.

show cdp run

Syntax Description

This command has no arguments or keywords.

Example

This command displays the CDP configuration:

```
show cdp run
CDP protocol is enabled ...
        broadcasting interval is every 60 seconds.
        time-to-live of cdp packets is 180 seconds.

        CDP is enabled on port eth0.
```

show collectorlog

To display the Wireless LAN Solution Engine's collector log, use the show collectorlog command.

show collectorlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's collector log, one page at a time:

```
show collectorlog page
/var/adm/CSCOets/log/collector.log
2001/12/20 13:43:18 main HSECollector MESSAGE CollectorMain: Waiting
for databas
e to be ready
2001/12/20 13:43:21 main HSECollector MESSAGE CollectorMain: Database
is ready
SNMPThrPool: Instantiated ex.lib.snmp.lib.timer.DynamicThreadPool,  mi
```

```
n=15, max=48, maxIdleSecs=0
2001/12/20 13:43:29 main HSECollector MESSAGE ServletServiceModule:
Moxie Servle
t Engine is ready to receive requests
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableCleanupCommand=[VACUUM ]
2001/12/20 13:43:30 PeriodicSchedulerRun:FaultCleanup HSECollector
MESSAGE Colle
ctorDBUtils: DB.TableUpdateStatsCommand=[VACUUM ANALYZE ]
2001/12/21 10:39:52 Moxie Servlet Engine:Pooled Thread:1 HSECollector
MESSAGE Se
rvletContextAdaptor: Collector: init
```

show config

To display the system configuration, use the **show config** command.

show config

Syntax Description

This command has no arguments or keywords.

Example

This command displays the system configuration:

```
show config
hostname ex1
interface ethernet0 209.165.201.0 255.255.255.224 default-gateway
209.165.202.128
interface ethernet1 down
interface ethernet2 down
interface ethernet3 down
interface ethernet4 down
interface ethernet5 down
ip domain-name embu-doc
ip name-server 209.165.202.158
username admin epassword ************* privilege 15
```

show daemonslog

To display the Wireless LAN Solution Engine's daemons log, use the **show daemonslog** command.

show daemonslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's daemons log, one page at a time:

```
show daemonslog page
/var/adm/CSCOets/log/daemons.log
[dmgrDbg] getenv(PX_DBG)=NULL
[dmgrDbg] getenv(PX_MY_DEBUG)=NULL
[dmgrDbg] getenv(PX_MY_TRACE)=NULL
[dmgrDbg] getenv(PX_DBG_LEVEL)=NULL
[dmgrDbg][Thu Dec 20 13:42:53 2001]##### INFO ##### re-evaluate
DbgLevel=0x0
        ++>>it(1) = 8077978 <HSECollector>
        ++>>it(1) = 8077898 <HSEANIServer>
        ++>>it(1) = 8077428 <PostgreSQL>
        ++>>it(1) = 8077228 <WebServer>
        ++>>it(1) = 8077328 <Tomcat>
        ++>>it(1) = 80770d8 <ExcepReporter>
        ++>>it(1) = 8076fc8 <CDPbrdcast>
        ++>>it(1) = 8076e58 <PerfMon>
#!/bin/sh -v
#!/bin/sh -v

if [ "$NMSROOT" = "" ]; then
```

```
        NMSROOT=/opt/CSCOets
        export NMSROOT
fi

cd $NMSROOT
--More--
```

show dmgtdlog

To display the Wireless LAN Solution Engine's daemon manager log, use the **show dmgtdlog** command.

show dmgtdlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's daemon manager log, one page at a time:

```
show dmgtdlog page
/var/adm/CSCOets/log/dmgtd.log
Dec 20 13:42:56 ex dmgt[712]: #3001:TYPE=INFO:Using port: tcp/42340.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEC
ollector) "/bin/nice -n 19 /opt/CSCOets/bin/collector" pid=715.
Dec 20 13:42:56 ex dmgt[714]: #3007:TYPE=INFO:Started application(HSEA
--More--
```

show hseaccesslog

To display the Wireless LAN Solution Engine's Web access log, use the **show hseaccesslog** command.

show hseaccesslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web access log, one page at a time:

```
show hseaccesslog page
/var/adm/CSCOets/log/access_log
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET / HTTP/1.0" 302
276 "-" "Moz
illa/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:54 +0000] "GET
/perl/login-form.cgi HTTP/1.
0" 200 2268 "-" "Mozilla/4.76 [en]C-CCK-MCD   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET /icons/hse.gif
HTTP/1.0" 200
 5554 "http://209.165.201.0:1741/perl/login-form.cgi" "Mozilla/4.76
[en]C-CCK-MC
D   (Windows NT 5.0; U)"
209.165.200.224 - - [21/Dec/2001:10:38:55 +0000] "GET
/icons/left_top.gif HTTP/1.0
" 200 324 "http://209.165.201.0:1741/perl/login-form.cgi"
"Mozilla/4.76 [en]C-CC
K-MCD   (Windows NT 5.0; U)"
--More--
```

show hseerrorlog

To display the Wireless LAN Solution Engine's Web error log, use the **show hseerrorlog** command.

show hseerrorlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web error log, one page at a time:

```
show hseerrorlog page
/var/adm/CSCOets/log/error_log
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
Invalid command
 'secret', perhaps mis-spelled or defined by a module not included in
the server
 configuration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
Invalid command
 'line', perhaps mis-spelled or defined by a module not included in
the server c
onfiguration
[Thu Dec 20 13:43:00 2001] [error] (22)Invalid argument: <Perl>:
```

show hsesslaccesslog

To display the Wireless LAN Solution Engine's Web SSL log, use the **show hsesslaccesslog** command.

show hsesslaccesslog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's Web SSL log, one page at a time:

```
show hsesslaccesslog page
```

show import

To display an imported host file, use the **show import** command.

show import *hosts*

Syntax Description

hosts	Name of server that host files were imported from.

Example

This command displays the imported host file

```
show import ftpserver_1
```

show install logs

To display the software updates and images available on the configured repository, use the **show install logs** command.

show install logs [short | long] [page]

Syntax Description

short	Displays only the names of software updates and images on the configured repository
long	Displays the names and descriptions of software updates and images on the configured repository.
page	Displays command output one screen at a time.

Example

The following command displays the software updates and images available on the configured browser, one screen at a time:

```
show install updates page
2
NAME=EX-2.0a
```

show ipchains

To display the IP chains for the selected interface, use the **show ipchains** command.

show ipchains *eth<0-5>*

Syntax Description

eth<0-5>	Name of the interface port to be configured. Acceptable values are eth0-5.

Example

The following command displays the IP chains for the ethernet 0 interface:

```
show ipchains eth0
Chain ineth0 (1 references):
target     prot opt     source               destination
ports
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   telt
ACCEPT     tcp  ------  anywhere             ex.help     any ->   3345
ACCEPT     tcp  -y--l-  anywhere             ex.help     any ->   ssh
```

show hosts

To display your Wireless LAN Solution Engine's host file, use the **show hosts** command.

show hosts [page]

Syntax Description

page	Displays command output one screen at a time.

Example

The following command displays your Wireless LAN Solution Engine's host file one page at a time:

```
show hosts page
```

show maillog

To display the Wireless LAN Solution Engine's mail log, use the **show maillog** command.

show maillog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's collector log, one page at a time:

```
show maillog page
/var/log/maillog
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: from=root, size=307, cla
ss=0, pri=30307, nrcpts=1, msgid=<200112210402.EAA11643@ex.help>, rela
y=root@localhost
Dec 21 04:02:06 ex sendmail[11660]: EAA11643: SYSERR(root): Cannot exe
c /usr/bin/procmail: No such file or directory
Dec 21 04:02:06 ex sendmail[11643]: EAA11643: to=root, ctladdr=root (0
/0), delay=00:00:06, xdelay=00:00:00, mailer=local, stat=Operating
system error
```

show proc

To display the Wireless LAN Solution Engine's active process statistics, use the **show proc** command.

show proc [page]

Syntax Description

page	Displays command output one screen at a time.

Example

The following command displays the Wireless LAN Solution Engine's active process statistics one page at a time:

```
show proc page
PID     ELAPSED    SZ                  STARTED TTY  COMMAND
    1    22:29:10   277 Thu Dec 20 13:42:29 2001 ?    init
    2    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kflushd
    3    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kupdate
    4    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kpiod
    5    22:29:10     0 Thu Dec 20 13:42:29 2001 ?    kswapd
    6    22:29:03     0 Thu Dec 20 13:42:36 2001 ?    kreiserfsd
   85    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   86    22:29:00     0 Thu Dec 20 13:42:39 2001 ?    kreiserfsd
   87    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   88    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
   89    22:28:59     0 Thu Dec 20 13:42:40 2001 ?    kreiserfsd
  208    22:28:57   290 Thu Dec 20 13:42:42 2001 ?    watchdog
  322    22:28:51   342 Thu Dec 20 13:42:48 2001 ?    idled
  510    22:28:51   290 Thu Dec 20 13:42:48 2001 ?    syslogd
  519    22:28:50   361 Thu Dec 20 13:42:49 2001 ?    klogd
  637    22:28:48   327 Thu Dec 20 13:42:51 2001 ?    crond
  651    22:28:48   286 Thu Dec 20 13:42:51 2001 ?    inetd
17076       18:23   364 Fri Dec 21 11:53:16 2001 ?     \_ in.telnetd
17077       18:23   575 Fri Dec 21 11:53:16 2001 0     |   \_ login
-----------more-----------
```

show repository

To display the status or the access log of a configured repository, use the **show repository** command.

show repository {status | access-log} [page]

Syntax Description

status	Displays the status of the local repository
access-log	Displays the access-log of the local repository

page Displays command output one screen at a time.

Example

This command displays the status of the configured repository:

```
show repository status
Repository Source: 171.69.212.146:9851
repository is running.
```

show route

To display the routes currently configured, use the show route command.

show route

Syntax Description

This command has no arguments or keywords.

Example

This command displays the currently configured routes

```
show route
Destination     Gateway Genmask         Flags Metric Ref    Use Iface
209.165.200.224 0.0.0.0 255.255.255.224 UH    0      0        0 eth0
209.165.200.225 0.0.0.0 255.255.255.224 U     0      0        0 eth0
209.165.200.254 0.0.0.0 255.255.255.224 U     0      0        0 lo
209.165.202.128 0.0.0.0 255.255.255.224 UG    0      0        0 eth0
```

show securitylog

To display the Wireless LAN Solution Engine's security log information, use the **show securitylog** command.

show securitylog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's security log, one page at a time:

```
show securitylog page
/var/log/secure
Dec 20 13:45:23 ex in.tftpd[1381]: connect from 209.165.200.224
Dec 20 13:45:27 ex in.tftpd[1383]: connect from 209.165.200.224
Dec 20 13:45:31 ex in.tftpd[1385]: connect from 209.165.200.224
Dec 20 13:45:35 ex in.tftpd[1387]: connect from 209.165.200.224
Dec 20 13:45:39 ex in.tftpd[1389]: connect from 209.165.200.224
Dec 20 13:45:44 ex in.tftpd[1391]: connect from 209.165.200.224
Dec 20 13:45:48 ex in.tftpd[1393]: connect from 209.165.200.224
Dec 20 13:45:52 ex in.tftpd[1395]: connect from 209.165.200.224
Dec 20 13:45:56 ex in.tftpd[1397]: connect from 209.165.200.224
Dec 20 13:46:00 ex in.tftpd[1399]: connect from 209.165.200.224
Dec 20 13:46:04 ex in.tftpd[1412]: connect from 209.165.200.224
Dec 20 13:46:27 ex in.tftpd[1424]: connect from 209.165.200.224
Dec 20 13:46:31 ex in.tftpd[1426]: connect from 209.165.200.224
Dec 20 13:46:35 ex in.tftpd[1428]: connect from 209.165.200.224
Dec 20 13:46:39 ex in.tftpd[1430]: connect from 209.165.200.224
Dec 20 13:46:43 ex in.tftpd[1432]: connect from 209.165.200.224
Dec 20 13:46:47 ex in.tftpd[1434]: connect from 209.165.200.224
--More--
```

show snmp-server

To display the Wireless LAN Solution Engine's SNMP configuration, use the **show snmp-server** command.

show snmp-server

Syntax Description

This command has no arguments or keywords.

Example

The following command displays the Wireless LAN Solution Engine's SNMP configuration:

```
show snmp-server
RW community string: private
        RO community string: public

        sysLocation: your site information
        sysContact: your contact information

        trap-forwarding is disabled
```

show ssh-version

To display the type of SSH enabled, use the ssh-version command.

show ssh-version

Syntax Description

This command has no arguments or keywords.

Example

This command displays the type of SSH that is enabled:

```
show ssh-version
SSH1, SSH2
```

show syslog

To display syslog information, use the **show syslog** command.

show syslog [page] [include *matchstring1* **[***matchstring2***]]**

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Usage Guidelines

Use this command to display syslog information.

To filter the command output to include only the records that contain the specified string(s) of characters, use the **include** option with one or two character strings to search for. If you include two strings, the command outputs only those records that contain both character strings.

Example

This command displays syslog information:

```
show syslog
Jun 20 16:04:23 ex syslogd 1.3-3: restart.
Jun 20 16:04:23 ex syslog: syslogd startup succeeded
Jun 20 16:04:23 ex kernel: klogd 1.3-3, log source = /proc/kmsg start.
Jun 20 16:04:23 ex kernel: Inspecting /boot/System.map-2.2.16-13bipse2
Jun 20 16:04:23 ex syslog: klogd startup succeeded
-----------more-----------
```

Related Command

interface

show tech

To display information necessary for Cisco's Technical Assistance Center to assist you, use the **show tech** command.

show tech [page]

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.

Example

This command displays system information necessary for Cisco's Technical Assistance Center to assist you.

```
show tech page
/bin/cat: /var/log/secure: Permission denied
Copyright (c) 1999-2000 by Cisco Systems, Inc.
Build Version (166) Mon Jun 11 16:56:23 PDT 2001
Linux/UID32 version 2.2.16-13bipsec.uid32 (gcc version egcs1
Uptime: 0 days 18 hours 35 mins

2 Ethernet interfaces
hostname ex
interface ethernet0 209.165.200.224 255.255.255.224 default-gateway
209.165.202.128
ip name-server 209.165.201.0
username admin epassword ************* privilege 15
eth0      Link encap:Ethernet  HWaddr 00:02:B3:35:FD:CC
          inet addr:209.165.200.224 Bcast:209.165.201.31
Mask:255.255.255.224
-----------more-----------
```

show telnetenable

To display the Wireless LAN Solution Engine's Telnet status, use the **show telnetenable** command.

show telnetenable

Syntax Description

This command has no arguments or keywords.

Example

The following command shows if Telnet is enabled or disabled:

```
show telnetenable
telnet enable for: ALL
```

show tomcatlog

To display the Wireless LAN Solution Engine's Tomcat log, use the **show tomcatlog** command.

show tomcatlog [page] | include *matchstring1 [matchstring2]*

Syntax Description

page	Displays command output one screen at a time. Press the Return key to display the next output screen. Press **Ctrl-c** to exit paged output and return to the command prompt.
include	Filters the command output to display only the records that contain the specified string of characters.
matchstring1	String of characters to search for in the command output.
matchstring2	(Optional) Another string of characters to search for in the command output.

Example

The following command displays the Wireless LAN Solution Engine's tomcat log, one page at a time:

```
show tomcatlog page
/var/adm/CSCOets/log/tomcat.log
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /examples )
2001-12-20 01:43:06 - ContextManager: Adding context Ctx( /admin )
Starting tomcat. Check logs/tomcat.log for error messages
2001-12-20 01:43:06 - ContextManager: Adding context Ctx(  )
getUIProperties(): unhandled error could be a bad ui.properties
```

```
java.lang.NullPointerException
        at java.io.Reader.<init>(Reader.java:68)
        at java.io.InputStreamReader.<init>(InputStreamReader.java:96)
--More--
```

shutdown

To shut down the system in preparation for powering it off, use the **shutdown** command.

shutdown

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use this command to shut down the WLSE in preparation for powering it off. All processes running on the WLSE will stop, and it will not respond until you power it off and back on.

You are prompted to verify the shutdown. Enter **yes** to continue, or **no** to cancel the shutdown.

Caution Never power the system off without running the **shutdown** command first. Doing so can destroy data and prevent the system from booting.

Example

This command shuts down the system:

```
shutdown
```

Related Commands

reload

snmp-server

To configure an simple network management protocol (SNMP) agent, use the **snmp-server** command.

snmp-server {community *community-name* **[RO|RW] | location** *sysLocation-info* **| contact** *sysContact-info***}**

no snmp-server {community *community-name* **| location | contact}**

Syntax Description

community	sets the community strings that permit access to the SNMP.
community-name	the community name string.
RO	read only.
RW	read / write.
location	sets the system location string.
sysLocation-info	the location string.
contact	sets the contact string.
sysContact-info	the contact string.

Example

This command sets an SNMP contact string:

```
snmp-server contact Dial System Operator at Beeper # 27345
```

ssh

To use SSH to connect to an external host, use the ssh command.

ssh [*options***]** *host* **[***command***]**

Syntax Description

options	Standard SSH options. For a list of these options, enter the **ssh** command without any arguments.
host	Name or IP address of host to which to connect.
command	Command for the external host to execute.

Example

Enter the following command to connect to an external host using SSH:

```
ssh 209.165.200.224
```

ssh-version

Use the ssh-version command to enable Secure Shell (SSH) 1, SSH 2, or both SSH 1 and SSH 2.

ssh-version {ssh1 | ssh2 | both}

Syntax Description

ssh1	Enables SSH 1
ssh2	Enables SSH 2
both	Enables both SSH 1 and SSH2

Example

This command enables ssh1:

```
ssh-version ssh1
```

telnet

To Telnet to an external host, use the telnet command.

telnet {*hostname* **|** *ip-address***} [***portnumber***]**

Syntax Description

hostname	Hostname of the external device.
ip-address	IP address of the external device.
portnumber	portnumber of the external device.

Example

Enter the following command to telnet to port 9851 of a system with the IP address 209.165.200.224:

```
telnet 209.165.200.224 9851
```

telnetenable

To configure Telnet access, use the **telnetenable** command.

telnetenable {enable [*ip-addresses* **|** *domains***] | disable | status}**

Syntax Description

enable	Enables Telnet access to the system.
disable	Disables Telnet access to the system.
status	Displays current access status.
ip-addresses	IP addresses of systems allowed Telnet access. If this argument is used, no other machines will be allowed access. Multiple IP address are allowed.
domains	Domains of systems allowed Telnet access. If this argument is used, machines with domains other than the specified domain will be denied Telnet access. Multiple domains are allowed.

Default

The default is **disable**.

Usage Guidelines

To enable Telnet access to the system for *all* IP source addresses, use the **telnetenable enable** command alone. To enable *specific* IP addresses, use the **telnetenable enable** command followed by the IP addresses.

Example

This command enables Telnet for all IP source addresses:

```
telnetenable enable
```

username

To create a new user account or change an account's properties, use the **username** command. Use the **no** form of the command to remove a user account.

username *name* **password** *password* **[privilege {0 | 15}]**

no username *name*

Syntax Description

name	Name of the user account to create or remove.
password	Specifies a password for the account.
password	The password for the account.
privilege	(Optional) Specifies the account privilege level.
0	Gives the account level 0 privileges. This is the default.
15	Gives the account level 15 privileges.

Usage Guidelines

Use the **username** command to change the properties of a user account. To assign a user CLI privilege level 15, use the **username** command. You cannot assign CLI privilege level 15 through the Web interface. Use the **no** form of the command to remove a user account. The default privilege level is 0 if you do not provide the privilege option.

For more information about managing user accounts and privilege levels, refer to Administering Users, page 5-60.

Example

This command creates a user account named user1 with password password1 and privilege level 15:

```
username user1 password password1 privilege 15
```

This command removes the user account:

```
no username user1
```

Maintenance Image Commands

This section describes the commands that are available when the system is booted from the maintenance image. For more information about the maintenance image, refer to the *Installation and Configuration Guide for the Cisco 1105 Wireless LAN Solution Engine*.

erase config

This command is identical to the level 15 **erase config** command. For a description, see the "erase config" section on page B-22.

fsck

To check and repair the filesystem, use the fsck command.

fsck

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **fsck** command to check and repair the filesystem. The command might prompt you for confirmation before making certain repairs.

Example

The following command checks and repairs the filesystem:

```
fsck
```

reload

This command is identical to the level 15 **reload** command. For a description, see "reload" section on page B-39.

A

access point Access points are wireless LAN transceivers that serve as the center point of a standalone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

B

bridge *See* wireless bridge.

C

CDP distance The CDP distance determines the depth of the discovery and applies to all seed devices. If CDP distance is 1, only the immediate neighbors of the seed device are discovered. If CDP distance is 2, devices A and B that are directly connected to the seed devices are discovered and the immediate neighbors of A and B are also discovered.

CLI The command line interface for administering the WLSE. You use the CLI through a console attached to the WLSE's console port or by opening a Telnet connection to the WLSE. CLI commands are described in the *User Guide for the CiscoWorks 1105 Wireless LAN Solution Engine*.

community strings Text strings that act as passwords to authenticate communication with devices that contain an SNMP agent.

E

EAP server Servers running extensible authentication protocol to provide dynamic, session-specific wireless encryption keys, central user administration. and authentication between clients and access points.

See also LEAP server.

exception A group of related faults.

L

LEAP server Light EAP server used by the Wireless LAN Solution Engine to combine centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.

See also EAP server.

N

nslookup The NSLookup tool is used to look up device or host information via the name server. You must enter a device name, not an IP address, to use this function. You must have a DNS server in order to look up network servers.

P

ping A common method for troubleshooting the accessibility of devices.

A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used. If ping fails, try using traceroute.

Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.

R

repository The Repository provides software update services to the Solution Engine. You can download software from the Repository and install it on the Solution Engine, and you can browse the available software versions on the Repository.

S

seed A CDP-enabled device used as a starting point for discovery. For example, by adding a seed device (or set of seed devices), the neighbors of the seed device are discovered using CDP.

SSID Service Set ID. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.

SSL Secure Socket Layer. Proves a secure connection between the WLSE and Web clients.

T

threshold A range within which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device.

traceroute This is a diagnostic tool that helps you understand why ping fails or why applications time out. Using it, can view each hop (or gateway) on the route to your device and how long each took.

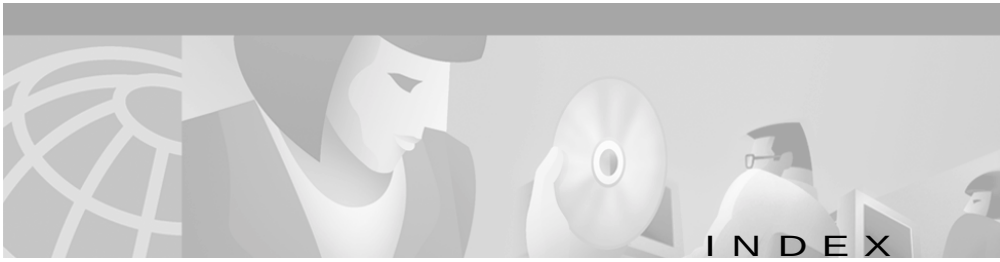
U

UTC Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

W

WEP keys Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.

wireless bridge Designed to connect two or more networks (typically located in different buildings). Bridges connect hard-to-wire sites, noncontiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. For functional flexibility, the wireless bridge may also be configured as an access point.



A

B

C

D

E

F

G

H

I

J

L

M

N

P

R

S

T

U

W